

TABLE OF CONTENTS

CHAPTER 1	Overview	Page 4
1.1	Purpose of the FOIPP Act.....	Page 5
1.2	Public Bodies Within the Scope of the Act	Page 6
1.3	Organizations Not Within the Scope of the Act	Page 6
1.4	Scope of the Act.....	Page 6
1.5	Records Covered by the Act	Page 7
1.6	Custody or Control	Page 8
1.7	Records Excluded from the Act.....	Page 9
1.8	Accessing Information	Page 15
1.9	Routine Disclosure of Information	Page 15
1.10	Practices for Routine Disclosure and Active Dissemination	Page 19
CHAPTER 2	Administration of the FOIPP Act	Page 23
2.1	Public Body – Roles and Responsibilities	Page 23
2.2	Delegation of FOIPP Responsibilities	Page 24
2.3	Province Wide Administration of the Act	Page 26
2.4	Liability, Sanctions and Penalties	Page 28
CHAPTER 3	Access to Records	Page 30
3.1	Who Has a Right of Access	Page 30
3.2	Receiving a FOIPP Request.....	Page 30
3.3	Processing a FOIPP Request	Page 43
3.4	Responding to a FOIPP Request.....	Page 64
CHAPTER 4	Exceptions to the Right of Access	Page 69
4.1	Overview.....	Page 69
4.2	Relationship to Other Acts	Page 74
4.3	Disclosure Harmful to Business Interests of a Third Party.....	Page 75
4.4	Disclosure Harmful to Personal Privacy	Page 83
4.5	Disclosure Harmful to Public or Individual Safety.....	Page 99
4.6	Confidential Evaluations.....	Page 102
4.7	Disclosure Harmful to Law Enforcement	Page 104
4.8	Intergovernmental Relations	Page 118
4.9	Cabinet Confidences	Page 122
4.10	Public Body Confidences.....	Page 125
4.11	Advice from Officials	Page 127
4.12	Economic and Other Interests of a Public Body or the Government of Prince Edward Island.....	Page 138
4.13	Testing Procedures.....	Page 143
4.14	Privileged Information	Page 144
4.15	Disclosure Harmful to Archaeological Sites, Heritage Places, Rare, Endangered or Vulnerable Life	Page 155

4.16	Information That Is or Will Be Published.....	Page 156
CHAPTER 5	Third Party Intervention and Notice	Page 159
5.1	Overview	Page 159
5.2	When Is Third Party Notification Required?	Page 159
5.3	How Is a Third Party Notification Process Carried Out	Page 160
5.4	Content of Third Party Notice.....	Page 162
5.5	Notice to Applicant	Page 162
5.6	Response from Third Party	Page 163
5.7	Notice of Decision	Page 163
5.8	Time Limits.....	Page 164
5.9	Time Limit Extension	Page 167
CHAPTER 6	Disclosure in the Public Interest	Page 169
6.1	Overview	Page 169
6.2	Disclosure	Page 170
6.3	Public Interest	Page 171
6.4	Determination of Public Interest.....	Page 172
6.5	Scope	Page 173
6.6	Notification	Page 173
6.7	Review	Page 174
6.8	Disclosure to the Commissioner	Page 175
CHAPTER 7	Protection of Privacy.....	Page 177
7.1	Overview	Page 177
7.2	Purposes of Collection	Page 179
7.3	Manner of Collection	Page 182
7.4	Accuracy and Retention.....	Page 192
7.5	Correction of Personal Information	Page 194
7.6	Protection of Personal Information.....	Page 199
7.7	Use of Personal Information	Page 201
7.8	Disclosure of Personal Information	Page 205
7.9	Consistent Uses	Page 227
7.10	Disclosures for Research or Statistical Purposes	Page 228
7.11	Disclosure of Information in Archives	Page 232
7.12	Exercise of Individual Rights by Other Persons	Page 235
CHAPTER 8	Information and Privacy Commissioner	Page 238
8.1	Overview.....	Page 238
8.2	Appointment	Page 238
8.3	Mandate and Powers	Page 241
8.4	Monitoring Role	Page 241
8.5	Provision of Advice	Page 241
8.6	Disclosure to the Commissioner	Page 241

8.7	Powers	Page 242
8.8	Access to Information	Page 242
8.9	Power to Disregard Requests	Page 243
8.10	Statements Provided to the Commissioner	Page 245
8.11	Protection from Liability	Page 246
8.12	Delegation of the Commissioner's Powers	Page 246
8.13	Reviews and Investigations	Page 246
8.14	Adjudicator Process	Page 254
8.15	Judicial Review	Page 255

APPENDIX

A.	FOIPP 30-day Process Chart.....	Page 256
B.	Record Search Form.....	Page 260
C.	Guide How to Search Outlook.....	Page 262
D.	Guide How to Search Groupwise...	Page 283
E.	FOIPP Delegation tool.....	Page 293

CHAPTER INTRODUCTION

Prince Edward Island enacted the *Freedom of Information and Protection of Privacy Act* (*FOIPP Act*) on November 1, 2002. This publication provides a comprehensive reference tool for the application of the *FOIPP Act*. The FOIPP Guidelines and Practices Manual will provide public bodies with detailed background and process information to help guide their decisions or take actions that will comply with the *FOIPP Act*. The Manual is adapted from Alberta's manual and suggests how the Act and its Regulations should be understood, taking into consideration the most significant decisions of Information and Privacy Commissioners. The manual also explains roles and responsibilities with respect to the administration of the Act and offers guidance on procedural matters.

All orders of the Commissioner are posted to the website (www.oipc.pe.ca). They provide insight into past decisions and consequences of these decisions as they relate to the Act.

The information found in this manual is provided for guidance and information purposes only. It should not be relied upon as a substitute for legal advice in any particular matter. Further, we cannot guarantee that all information is current or accurate as of the date of reading.

This manual is an evergreen document and is subject to revision without notice based upon changes in law and other best practices.

For more information contact:

Access and Privacy Services Office

Email – apso@gov.pe.ca

Telephone - 902 569 7590

CHAPTER 1

1.1 PURPOSE OF THE FOIPP ACT

The basic objectives of the FOIPP Act are to ensure that public bodies are open and accountable to the public by providing a right of access to records and by protecting the personal privacy of individuals.

Section 2 of the Act sets out five purposes.

A Right of Access to Records: The first purpose is to establish a right of access by any person to records in the custody or under the control of a public body, subject to limited and specific exceptions which are set out in the Act.

This right of access is the cornerstone of openness and accountability of public bodies and should be taken into account when making any decision about disclosing records in response to the FOIPP request.

The limited and specific exclusions and exceptions which are set out in the Act provide the only basis for refusing access to records and should always be interpreted with a view to giving as much access as possible to the records requested.

Protection of Personal Privacy: The second purpose is to control the manner in which a public body may collect personal information from individuals, the use that it may make of that information, and its disclosure of that information.

A Right of Access to an Individual's Own Personal Information: The third purpose is to create a right of access for individuals to personal information about them, again subject to limited and specific exceptions set out in the Act.

The exceptions should always be interpreted with a view to giving an individual as much as access as possible to their own personal information.

A Right of Correction: The fourth purpose is to allow individuals a right to request corrections to personal information about themselves that is held by a public body.

Independent Review of Decisions: The fifth purpose is to provide for the independent

review of decisions made by public bodies under the Act and for the investigation of complaints. Independent review is provided by the Information and Privacy Commissioner.

1.2 PUBLIC BODIES WITHIN THE SCOPE OF THE ACT

The FOIPP Act applies to public bodies. A public body is defined in **section 1(k)** of the Act as:

- A department, branch or office of the Government of Prince Edward Island;
- An agency, board, commission, corporation, office, or other body designated as a public body in the FOIPP Regulations;
- The Executive Council Office; or
- The offices of the Auditor General, the Clerk, Clerk Assistant and Sergeant-at-Arms, the Chief Electoral Officer, the Information and Privacy Commissioner, or the Conflict of Interest Commissioner
- **A local public body**

1.3 ORGANIZATIONS NOT WITHIN THE SCOPE OF THE ACT

Section 1(k) specifically excludes the following from the Act:

- The office of the Speaker of the Legislative Assembly;
- The office of a Member of the Legislative Assembly; or
- The Court of Appeal of Prince Edward Island, the Supreme Court of Prince Edward Island or the Provincial Court of Prince Edward Island

Since government departments are public bodies and the Executive Council Office is a public body, but the office of a Member of the Legislative Assembly is not, some records of Member of the Executive Council (Cabinet Members) will fall within the scope of the Act and others will not. The records of Members of the Executive Council that relates to their duties in Cabinet and in the administration and operation of a public body are within the scope of the Act, but records that relate to their duties as MLAs are not.

Section 1 of the Act contains a number of definitions that set out which bodies are and are not public bodies for the purposes of the Act. Bodies that are subject to the Act have statutory duties with regard to access to information and protection of privacy. Section 4 of the Act is concerned with defining which records are subject to the Act.

1.4 SCOPE OF THE ACT

Some public bodies have routine procedures regarding disclosure of information and records. The FOIPP Act is in addition to and does not replace these existing procedures (**section 3(a)**). However, any routine disclosure of personal information by public bodies must be in compliance with Part 2 of the Act.

Routine disclosure of information is discussed in more detail in section 1.9 of this chapter.

The Act does not affect access to records deposited in the Public Archives and Records Office before the Act came into force (**section 3(b)**). The Act does not limit the information otherwise available by law to a party to legal proceedings (**section 3(c)**).

Legal proceedings are activities governed by rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgement or a court or a ruling by a tribunal. **Section 3(c)** means that the Act does not prevent or limit the use of legal processes such as examination for discovery to gather information about a party in a lawsuit.

If a person involved in a criminal or civil legal action makes a FOIPP request to a public body for records relating to the case, that request should be processed as a FOIPP request, applying the provisions of the Act.

If an action proceeds to discovery, or if some other legal procedure is invoked to obtain disclosure of records, the rules governing that legal procedure will apply. The access provisions of the FOIPP Act are applicable only to requests made under the FOIPP Act and not to other legal processes. It is common to have both processes going on at the same time.

The provisions of the Act do not override the power of any court or tribunal to compel a witness to testify or to compel the production of documents (**section 3(d)**). The Act does not prohibit the transfer, storage or destruction of a record in accordance with an enactment of Prince Edward Island or Canada (**section 3(e)**). This permits the orderly disposition of records by public bodies in accordance with records retention and disposition schedules.

1.5 RECORDS COVERED BY THE ACT

The Act applies to all the records *in the custody* or *under the control* of a public body, including court administration records (**section 4(1)**).

Definition of Record

Record means a record of information in any form, including, electronic form, but does not include a mechanism or system for generating, sending, receiving, storing or otherwise processing information. (**section 1(l)**).

Definition of Personal Information

The Act defines *personal information* as recorded information about an identifiable individual, including, but not limited to:

- The individual's name, home or business address or home or business telephone number.
- The individual's race, national or ethnic origin, colour or religious or political beliefs or associations.
- The individual's age, sex, marital status or family status.
- An identifying number, symbol or other particular assigned to the individual.
- The individual's fingerprints, **other biometric information**, blood type, **genetic information** or inheritable characteristics.
- Information about the individual's health and health care history, including information about a physical or mental disability.
- Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given.
- Anyone else's opinions about the individual.
- The individual's personal views or opinions, except if they are about someone else (**section 1(i)**).

1.6 CUSTODY OR CONTROL

A public body has *custody* of a record when the record is in the possession of the public body.

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

Some indicators that a record may be in the custody or under the control of a public body are as follows:

- The record was created by an officer, employee or member of the public body;

- The record was created by an outside contracted consultant for the public body;
- The record is specified in a contract as being under the control of a public body;
- The record is in the possession of the public body;
- The record is closely integrated with other records of the public body;
- The content of the record relates to the public body's mandate and functions;
- The public body has the authority to regulate the record's use and disposition;
- The public body has relied upon the record to a substantial extent; or
- A contract permits the public body to inspect, review or copy records produced, received or acquired by a contractor as a result of a contract.

The most common situation where a public body may have control, but not custody, of a record is in the case of contracted services. The record is created by and in the possession of the contractor, but the public body has set out some rights of access in the contract. For example, general clauses such as the following are often found in contracts:

- The contractor will keep and make available to the public body, upon request, records in a form that will allow the public body to determine that the services are being provided, upon the request of the public body.
- The contractor will furnish such information and particulars, as required by the public body, concerning the services and the care and progress of persons receiving services, upon the request of the public body.

In such cases, records used by the public body to monitor or inspect the delivery of the services would be deemed to be under its control.

Administrative records relating to the business of a contractor would not normally be considered to be under the control of a public body unless this was specifically stipulated in the contract. If a contractor deals with a subcontractor, but a public body does not exercise any rights in regard to the records relating to the work of the subcontractor, those records will not be under the control of a public body.

All public bodies should review their contracting practices to ensure that they adequately take the FOIPP Act into account. There may be situations, such as a records storage centre, where both control and custody lies with the public body storing the records and not with the organization offering the storage service.

1.7 RECORDS EXCLUDED FROM THE ACT

A limited number of types of records in the custody or under the control of public bodies are excluded from the application of the Act. These are as follows.

Certain Categories of Court and Judicial Records (section 4(1)(a))

Information in a court file, a record of a judge of the Supreme Court of Prince Edward Island or the Provincial Court of Prince Edward Island, a record of a prothonotary, a record of a sitting justice of the peace, a judicial administration record or a record relating to support services provided to a judge is not within the scope of this Act.

The term *judicial administration record* is defined in **section 4(2)** of the Act to mean a record containing information relating to the scheduling of judges and trials, the content of judicial training programs, statistics of judicial activity prepared by or for a judge, and any record of a judicial council.

Draft Judicial or Quasi-Judicial Decisions (section 4(1)(b))

A personal note, communication or draft decision created by or for a person who is acting in a judicial or quasi-judicial capacity is not within the scope of the Act.

This exclusion applies to communications between the members of the judicial or quasi-judicial body themselves, and between members and support staff, when these communications relate to the judicial or quasi-judicial functions of the body. The exclusion does not apply to decisions or reasons of the judicial or quasi-judicial body, although another exclusion or exception may apply to those records.

A *personal note* of a member of a judicial or quasi-judicial tribunal is one intended solely for the use of the person who wrote it.

The following criteria, which is not exhaustive, should be reviewed in determining whether a body is acting in a “judicial” or “quasi-judicial” capacity:

- Is there anything in the language in which the function is conferred or in the general context in which it is exercised that suggests that a hearing is contemplated before a decision is reached?
- Does the decision or order directly or indirectly affect the rights and obligations of persons?
- Is an adversarial process involved?
- Is there an obligation to apply substantive rules to many individual cases rather than, for example, an obligation to implement social and economic policy in a broad sense?

No one factor is decisive, and it will be necessary to consider the legislation under which a decision is made to see whether the rules of natural justice apply. The nature of the issue

to be decided and the importance of the decision for those affected should also be examined.

Records of an Officer of the Legislature (section 4(1)(c))

A record that is created by or for or is in the custody or under the control of an Officer of the Legislative Assembly, and relates to the exercise of that officer's functions under an enactment of Prince Edward Island, is not within the scope of the Act.

Operational files and correspondence of the Auditor General, the Clerk, Clerk Assistant and Sergeant-at-Arms, the Chief Electoral Officer, the Information and Privacy Commissioner, and the Conflict of Interest Commissioner are excluded from the coverage of the Act.

Correspondence to and from these offices is excluded regardless of where the files or correspondence are located, including letters, **email messages** and draft reports in the custody of a public body. It also includes records created by employees and contractors for these officers.

It is important to note that the administrative files of these legislative offices are subject to the Act, including personnel information, contracts and general office management records.

Records of the Conflict of Interest Commissioner (section 4(d))

Records created by or for or are in the custody or under the control of the Conflict of Interest Commissioner relating to any advice about conflicts of interest, whether or not the advice was given under the *Conflict of Interest Act* are excluded from the Act.

A Question to be used on an Examination or Test (section 4(1)(e))

A question to be used on an examination or test is not within the scope of the Act. This exclusion applies to questions that are to be used in the future. It also includes question banks from which questions are to be selected for future tests. The exclusion does not apply to test banks containing tests administered in the past which might be used as a

source of future questions for tests. Questions that were used in previous tests, but which will not be used again, are subject to the Act.

Archival Materials (section 4(1)(f))

Material that has been deposited in the Public Archives and Records Office or the Archives

of a public body by or for a person or entity other than a public body is not within the scope of the Act.

Individuals, corporations, labour unions, churches, and other groups may place collections of papers in the Public Archives and Records Office or the Archives of a public body.

These materials may continue to be owned by the depositing body or may be given to the archives. These records are not subject to the Act.

NEW: Also not within the scope of the Act (f.1) published works collected by a library of a public body in accordance with the library's acquisition of materials policy.

Records Relating to an Ongoing Prosecution (section 4(1)(g))

The Act does not apply to a record relating to a prosecution, if all proceedings in respect of the prosecution have not been completed. Prosecution records are excluded until the appeal period has expired, and, in a case where Crown counsel has stayed a criminal prosecution, until the one-year period from the stay has expired.

The exclusion here is to permit a legal proceeding to take place uninhibited by FOIPP requests. However, the FOIPP Act does apply to the records involved before the proceeding takes place, and after any stay or appeal period has expired. See also Chapter 4.7 of this publication for records relating to the exercise of prosecutorial discretion.

Public Registries (section 4 (1)(h))

The Act does not apply to a record made from information in:

- A Registry of documents relating to personal property;
- The office of the Director of Corporations;
- In the office of the Registrar of Deeds;
- An office of a division registrar, district registrar, or the Office of the Director as defined in the *Vital Statistics Act*; or
- In a registry operated by a public body, if that registry is authorized or recognized by an enactment and public access to the registry is normally permitted;

This provision recognizes that there are a number of public registries that record information for particular purposes and have been recognized as important to the functioning of a variety of social, economic and regulatory activities. These include transfer of land, corporate ownership and the securing of debt. Most public registries contain personal information that would otherwise be protected from disclosure. However, the disclosure of this information, and procedures for obtaining access to the information,

are already regulated by law. The exclusion applies to any record made from such a registry, whether in the custody of the public body operating the registry or of another public body. The exclusion applies only to the records. The Act still applies to the collection of the information.

Section 4(1)(h.1); Personal or Constituency records of an elected or appointed member of a public body:

A personal record or constituency record of an elected or appointed member of a public body is not within the scope of the Act. For example, personal records of a school board trustee relating to their private business activities do not fall within the scope of the Act. This exclusion does not apply to personal information in records related to the mandate and functions of the governing body or related to the member in their capacity as an employee.

A personal record or constituency record of an elected or appointed member of a local public body

Personal or Constituency Records of a Member of the Executive Council (section 4(1)(I))

A personal record or constituency record of a member of the Executive Council is not within the scope of the Act. This means that records that relate to the duties of a member of the Executive Council while acting as an MLA are excluded from the scope of the Act, but records that relate to duties in Cabinet and in the administration and operation of a public body are within the scope of the Act.

Record of the Speaker or an MLA that is in the Custody or Control of the Legislative Assembly Office (section 4(1)(j))

A record created by or for the office of the Speaker of the Legislative Assembly or the office of a Member of the Legislative Assembly is not within the scope of the Act.

Correspondence among Ministers, MLAs (section 4(1)(k))

This provision excludes certain records created by or for one of the two following classes of individuals:

- . A member of the Executive Council; or
- . A member of the Legislative Assembly.

In order to be excluded from the scope of the Act, the record must also have been sent, or be intended to be sent, to another Minister or MLA, as defined above. As such, there are two requirements to meet before this narrow exclusion can be applied to records:

1. The record was created by one of the above two classes of individuals or created on behalf of one of the above two classes of individuals. And,
2. That record was sent or intended to be sent to member of the Executive Council or a member of the Legislative Assembly.

Attachments to records that fall under this exclusion are not automatically excluded. Attachments must individually fulfill the requirements of this provision.

This provision recognizes situations such as those that may arise with committees, where information that may eventually form part of the discussions of the Executive Council or one of its committees is exchanged and is the subject of discussion, consideration, advice and recommendation. The exclusion extends to copies of such records sent to others, including officials in a public body.

Credit Union Records (section 4(1)(l) and (m))

The following records relating to credit unions are excluded from the Act:

- Records relating to the business or affairs of Credit Union Central of Prince Edward Island, the Credit Union Deposit Insurance Corporation, a credit union or a dissolved credit union.
- Records relating to an application for incorporation as a credit union.

The records must be obtained or produced in the course of administering or enforcing the *Credit Unions Act* or the regulations under it, and must relate to a transaction that is not a non-arm's length transaction as described above.

A non-arm's length transaction is defined in **section 4(3)**, for the purpose of this provision, as any transaction that has been approved by:

- The Executive Council or any of its committees; or
- A member of the Executive Council.

Personal Health Information (section 4(1)(n))

Some health records have been excluded from the FOIPP Act. They include personal health information as defined in the *Health Information Act* R.S.P.E.I. 1988, Cap. H-1.41, that is in the custody or control of a public body that is a custodian as defined in the *Health*

Information Act.

Dealing with Excluded Records

Where an excluded record is part of records responsive to a request and will not be disclosed, the public body should indicate that the record, or part of the record, is excluded.

Dealing with Paramount Legislation

The FOIPP Act will prevail in the event of an inconsistency or conflict with another enactment, unless another Act or a regulation under the FOIPP Act expressly states that the other enactment prevails.

If a provision of another Act or Regulation is paramount over the FOIPP Act, then the FOIPP Act does not apply, *to the extent of the conflict or inconsistency*.

The relationship of the FOIPP Act to other legislation is discussed further in Chapter 4.2 of this publication.

1.8 ACCESSING INFORMATION

There are three methods for the public to gain access to the information and records of public bodies:

- Routine disclosure in response to inquiries and requests for information
- Active dissemination by the public body
- FOIPP requests

Routine disclosure and active dissemination, which are described in **sections 1.9 and 1.10** of this chapter, will likely satisfy most of the information needs of members of the public. The FOIPP process is in addition to and does not replace existing procedures for access to information (**section 3(a)**).

Public bodies will find it beneficial to undertake continuous review of their processes and channels for providing information and records to the public to ensure that they are operating effectively and in support of the FOIPP Act.

1.9 ROUTINE DISCLOSURE OF INFORMATION

All public bodies provide routine access to information to members of the public. The Act does not replace existing procedures for providing access to information (see section 1.4 of this chapter). Most information should be made available as a matter of ordinary business.

FOIPP requests are time-consuming and expensive to process. The more information that can be released to the public or interested segments of the public through normal channels, the more effective a public body will be both in administering its programs and activities and in meeting the spirit of the FOIPP Act.

Indeed, the Act is intended to strengthen these informal access rights by encouraging routine disclosure. FOIPP requests should be the last resort for someone seeking information from a public body.

There are a number of ways that public bodies currently make information accessible through regular channels, without the need for a FOIPP request.

Answers to Particular Questions

Public bodies handle a large number of inquiries from members of the public seeking the answer to a question rather than asking for access to records.

Occasionally, a person will combine a question with a request for records. To the greatest extent possible, public bodies should continue to deal with these questions without a FOIPP request through information offices or the appropriate program area and approval process. Only when it becomes clear that the request involves records that cannot be released outside the FOIPP process, such as personal information about a third party, should the person be referred to the formal process under the FOIPP Act.

Reports and Publications

Much information is available in reports and publications through government websites and through various program information offices. These may either be available free of charge or for a price.

In order to meet the spirit of the Act, public bodies should maintain listings of material they publish through their communications office, library, information resource center or the FOIPP Analyst.

Similar practices should also be adopted for computer databases and information services that are available on various electronic networks. In planning these information dissemination channels, public bodies should consider how such information may be made more available through library and community networks, as well as larger networks, such as the Internet.

Records Available Without a FOIPP Request

Section 73(1) of the Act provides that public bodies may specify categories of records in their custody or under their control that will be made available to the public without a request for access under the Act. In this way, public bodies can take a proactive approach by setting up channels for the release of information and identifying records that are available without a FOIPP request. This approach supports efficient administration, maximizes the use of resources and promotes more openness and accountability in a public body.

Routine disclosure, in response to a routine inquiry or request, occurs when access to a record can be granted without a request under the FOIPP Act.

Active dissemination occurs when information or records are periodically released, without any request, under a program or release strategy. Active dissemination is best used where there is a strong and constant demand for information by the public.

Quite often such information is now being disseminated through database networks or Internet services **including Open Data and Open Government platforms**. Information made available by active dissemination may lend itself to pricing through subscription or dissemination charges or to cooperative dissemination ventures with public organizations or the private sector.

Public bodies might consider the appropriateness of routine disclosure in the following situations:

- Disclosure is mandated by another statute or regulation;
- **Section 37** of the FOIPP Act permits disclosure;
- No exceptions to access apply to record;
- Any exceptions that apply to a class of records are not mandatory exceptions, and the public body, if it received a request for the particular class of records, would not invoke any discretionary exceptions; or
- Exceptions do apply to a class of records but the sensitive information can easily be severed from the other information and that other information may be routinely disclosed.

Routine Disclosure has numerous advantages:

1. The public will be better served and better informed through targeted information releases that serve overall program objectives.
2. Disclosure in response to routine inquiries and active dissemination promote cost-effective management of public resources.
3. It allows staff to provide information to the public in an efficient manner.

In addition, **section 73(2)** enables a public body to set fees for the provision of information in this manner, unless records can otherwise be accessed without a fee. If a request cannot

be satisfied entirely through routine disclosure, then the request may be dealt with in part through routine disclosure and in part through the FOIPP request process. An example would be a request that requires all records related to a topic rather than just the finished report.

Public bodies should provide guidelines to its staff so that they are aware of the types of information available for release without a FOIPP request. Staff with questions regarding routine disclosure should seek advice from a FOIPP Analyst. Analysts should monitor requests received by the public body to determine subject areas and records that may qualify for access without a FOIPP request or through active dissemination.

Chapter 3 of this publication deals with the processing of FOIPP requests.

Special Conditions for Personal Information

Personal information requires special consideration when making decisions about disclosure through routine channels.

Public bodies may be able to identify categories of records containing personal information that may be routinely made available only:

- To the individual the information is about; or
- To the individual's legal representative (**section 71(1)**).

Designation of categories of personal information for this limited form of routine disclosure does not require any specific legislative authority.

The public body must, when providing routine disclosure of personal information:

- Verify the identity of the person to whom the information is disclosed.
- Ensure that any person exercising the rights of an individual under **section 71** of the Act provides appropriate written evidence of their right to exercise that individual's rights under the Act.

Each public body should designate categories of personal information for routine disclosure to the individual. Where there is considerable demand for a particular type of record, for example client files, a routine process, with fewer processes and approval requirements, can save a public body considerable time, effort and resources. However, when providing routine access public bodies must ensure that disclosure of personal information of other individuals does not occur.

Section 73(2) permits public bodies to set a fee for providing records to individual

members of the public unless the records can be accessed without a fee. If a process for dealing with requests for information outside the FOIPP Act is put in place, individuals who make FOIPP requests can be referred to the routine process.

However, if there are two processes for obtaining access to information, such that a public body will provide routine access by individuals to their own files in addition to providing access in response to a FOIPP request, then the public body should advise individuals of the two processes. Public bodies should ensure that individuals are aware of both their statutory rights under the Act and the availability of any other method of access.

Where two processes exist, a public body meets its duty to assist an applicant under **section 8(1)** only if it informs the applicant that such a dual process is in place.

1.10 PRACTICES FOR ROUTINE DISCLOSURE AND ACTIVE DISSEMINATION

A major challenge for public bodies is to provide information and related client services to the public in a cost-effective fashion. To help satisfy this demand and foster more open public administration, the following practices to support routine disclosures have been developed.

These practices are based on the concepts of *routine disclosure* and *active dissemination*, as defined in **section 1.8** of this chapter.

Review of Information Holdings

In starting to establish a system of routine disclosure and active dissemination, it is necessary to review the records of the public body to determine where the concepts may apply.

Examples of release and dissemination include:

- Release of particular information whenever a member of the public requests it as part of the service being offered.
- Use of public information centres to provide information services, including services by mail and fax.
- Use of reference databases to answer queries from clients.
- Publication of self-browse and self-service database services.
- Distribution of databases to libraries and other public facilities or use of private sector information services to make popular government databases available.

- Use of the Internet and other public networks to distribute government records and information.

A list of public information sources for the public body should be prepared, kept up-to-date and distributed to all staff who deal with inquiries from the public. Such information should not need to be dealt with under the access provisions of the FOIPP Act.

Coordinating Committee

Where a public body is large or decentralized, it may be advantageous to develop a network of contacts in program and administrative areas or in its various institutions.

This may be built into a coordinating group that is mandated to develop a corporate policy on routine disclosure and **pro**-active dissemination and to help implement routine disclosure practices.

Members of such a group might include:

- Interested individuals from program areas with records that may well qualify for routine disclosure and **pro**-active dissemination.
- A communications officer interested in information release and dissemination.
- A representative of the records and information management practices area in the public body, who has a good grasp of the types of records held by the public body.
- A representative from the information technology area, who understands how the public body can use new information networks to release and disseminate information.
- A FOIPP Analyst who understands how routine disclosure and pro-active dissemination can assist the public body in dealing with the demands of the FOIPP Act.

Either the FOIPP Analyst or the Committee should develop a corporate policy on routine disclosure. Information about what is available routinely from the public body should be made available to client groups and to the public.

Review of Inquiries

The FOIPP Analyst or the committee should review the types of requests for information currently made to the public body to determine whether these can be met through either routine disclosure or pro-active dissemination.

The objective should be to respond to as many requests as possible outside the Act. This should involve an ongoing monitoring and review of FOIPP requests to determine whether requests of a particular nature can be handled under routine disclosure practices.

Review of Records

There is also a need to review the record holdings of the public body to determine which records not currently subject to routine disclosure or pro-active dissemination may qualify for such procedures. Special attention should be paid to the categories of records set out in **section 1.9** of this chapter.

Every jurisdiction that has implemented freedom of information legislation has found that there has been considerable ongoing demand for contracts, travel claims, major reports and plans, internal audits, tax and regulatory rulings, and inspection records, among other types of information. Attention should be given to these types of records for the application of routine disclosure or pro-active dissemination. In some instances, records may have to be written and prepared in a different way to facilitate access. For example, reports might be written in a more structured way, such that recommendations or personal information can easily be severed and the remainder of the record made public. Where this is necessary, the public body should establish standards for the creation of these types of documents and ensure that staff are familiar with them.

Delegation of Authority

The public body should delegate authority for all routine disclosure to the program area that collected, compiled or created the information. The program area or organization should, complying with the policies of the public body, establish mechanisms for the rapid and effective release of the information.

In the case of pro-active dissemination, the program area should be delegated the responsibility and accountability for establishing a dissemination process. The FOIPP Analyst can provide assistance and advice in establishing these processes including monitoring of their effectiveness in dissemination of information.

The public body should provide a list of all records subject to routine disclosure and pro-active dissemination to all employees of the public body. Identified employees should be trained to assist the public when a request is made for a record subject to routine disclosure or pro-active dissemination. Where it is unclear if a record falls within these categories then the employees should be able to refer the requestor to the appropriate source.

Creation of New Records

The corporate policy on routine disclosure and **pro**-active dissemination should ensure that the FOIPP Analyst is consulted when there are plans to create new types of records within the public body. This consultation should determine whether or not any of these new records could be subject to routine disclosure or **pro**-active dissemination.

Consideration should be given, where possible, to modifying standard records by removing segments that would be subject to mandatory exceptions. For example, if a record contains both general information and personal information, but the main purpose of the record is to provide general information, then practices can be put in place to move personal information onto a separate page or suppress the fields for personal information in an electronic record. This may make the record available for either routine disclosure or active dissemination.

Channels for Pro-active Dissemination

Pro-active dissemination can take many forms. As indicated above, a public body may have an information centre for clients where information can rapidly be gathered and sent to clients, by mail, fax or through electronic networks. Information may also be routinely made available in a public reading area.

Public bodies can establish Internet sites or on-line databases where interested citizens can obtain information either through an intermediary, or by direct on-line access if they have the necessary equipment and expertise. In other instances, public bodies can use other public or private agencies, including libraries or non-profit organizations that are part of their clientele, or general information services to distribute information on their behalf.

All **pro-active** dissemination projects involve some investment by public bodies, and these costs have to be balanced against improved services to the public. Sometimes, public bodies will want to charge fees or collect revenues from the licensing of databases to private electronic publishing services. When considering **pro-active** dissemination of electronic products, public bodies should, whenever appropriate and within budgetary constraints, consider using public and local networks such as the internet.

CHAPTER 2

Administration of the FOIPP Act

2.1 PROVINCE WIDE ADMINISTRATION OF THE ACT

Minister Responsible for FOIPP

The Lieutenant Governor in Council designates the Minister responsible for the Act by Order in Council. The Attorney General is the designated Minister with overall responsibility for the general administration of the Act across the province, including preparation and submission of amendments to the FOIPP Act and FOIPP Regulations and providing guidance about FOIPP.

Access and Privacy Services Office (APSO)

The Access and Privacy Services Office supports all aspects of the implementation and administration of the legislation across all public bodies.

The Access and Privacy Services Office provides public body clients with the following services and products:

- The development and distribution of regulations, policies and guidelines where appropriate or needed to assist public bodies in administering the legislation.
- Advice and guidance on the interpretation, implementation and operation of the Act and Regulations.
- Regular posting and distribution of updated FOIPP legislation and policies, as well as orders made public by the Information and Privacy Commissioner and other information - both in print and on the FOIPP web page on the PEI Government website.
- A tracking system for FOIPP requests.
- Organization of FOIPP training sessions and seminars.

Production of publications to enable FOIPP Analysts, key contacts and others in **designated** public bodies to remain up-to-date on issues and trends in the fields of freedom of information and the protection of privacy.

Information and Privacy Commissioner

The Information and Privacy Commissioner is an Officer of the Legislature who is independent of government. The Commissioner is responsible for providing an independent review of decisions made under the Act and issues orders in that capacity.

The Commissioner reports annually to the Speaker of the Legislative Assembly on the operation of the legislation (**section 59**).

The powers of the Commissioner and the role of the Office of the Commissioner are discussed in Chapter 8 of this publication.

2.2 PUBLIC BODY – ROLES AND RESPONSIBILITIES

Head of a Public Body

The head of each public body is responsible and accountable for all decisions made under the FOIPP Act that relate to that public body. The following are heads of public bodies:

- In the case of a department, branch or office of the Government of Prince Edward Island, the head is the member of the Executive Council who presides over the public body (**section 1(d)(i)**).
- In the case of an agency, board, commission, corporation, office or other body designated as a public body in **Schedule 1** of the FOIPP regulations, the head is the person designated by the Minister responsible for that public body. If a head is not so designated, the person who acts as the chief officer and is charged with the administration of the body is the head (**section 1(d)(ii)**).
- In any other case, the head is the chief officer of the public body (**section 1(d)(iii)**).

FOIPP Analyst

Each public body should have a key contact person who can deal with FOIPP matters. This function is performed by the FOIPP Analyst. The FOIPP Analyst is responsible for

overall management of the freedom of information and protection of privacy function within a public body. Depending on the size and resources of the public body, the Analyst may carry out their responsibilities on a full-time or part-time basis. APSO will assign FOIPP Analysts to support department's branches and or offices of the Government of PEI.

The FOIPP Analyst's office should provide the focal point for freedom of information and protection of privacy expertise within the public body. Details of the responsibilities of this office throughout this publication represent a typical delegation of tasks. Public bodies may find that a different distribution of responsibilities is appropriate for them. The responsibilities might include:

- Implementing policies, guidelines and procedures to manage the public body's compliance with the provisions of the Act.
- Providing advisory services to the staff of the public body.
- Developing and delivering training programs on freedom of information and privacy protection within the public body and coordinating participation in FOIPP courses offered by the Government of Prince Edward Island.
- Informing the public body's clients, and all those with which it does business or provides services, about the Act.
- Advising senior management on information that can be released without a FOIPP request.
- Managing the FOIPP request process for the public body, which may include:
 - Assisting applicants.
 - Assigning requests to program areas.
 - Monitoring and tracking the processing of requests.
 - Meeting time limits and notification requirements.
 - Considering representations from third parties.
 - Calculating fee estimates and collecting fees.
 - Reviewing preliminary recommendations from program areas, sections or organizations about the release of records and proposals for severing information.
 - Making final recommendations on responses to requests.
 - Responding to applicants.
- Ensuring that the privacy protection measures in **Part 2** of the Act are implemented and carried out on an ongoing basis.
- Coordinating any negotiations, mediations, inquiries, investigations, and audits with the Office of the Information and Privacy Commissioner.
- Ensuring consistency in the application of other Acts and regulations which relate to the prohibition or restriction on the disclosure of information (**section 5**).
- Reporting as required to the Ministry responsible for FOIPP on the operation of the

Act.

- Maintaining a list of the public body's affiliated agencies for the purposes of **Schedule I** of the FOIPP Regulations.
- Consulting with the Ministry responsible for FOIPP regarding any legislative developments or amendments in other legislation that might relate to FOIPP.

Communications

In public bodies with a public relations area, communications staff may have a direct role in the freedom of information and protection of privacy function. Release of information in response to an access request should be coordinated with the overall flow of information to the public.

Where sensitive issues are involved, public bodies may wish to have a communications strategy in place when FOIPP disclosures take place.

Records and Information Management

The records and information management function within a public body is a major support for effective administration of the FOIPP Act. The same is true of the information technology function relating to the control of electronic databases and records.

Each public body should coordinate its efforts for managing, administering, controlling, providing security for, and preserving all its records. This includes electronic data and information, publications and other reports in its custody or under its control. This will ensure that the public body can meet its requirements under the Act.

Records and information management supports the FOIPP Analyst in:

- Establishing and maintaining an adequate level of information control to ensure that all records can be located and retrieved within the required time limits.
- Establishing and maintaining information management systems for the public body that comply with the Act's privacy protection provisions.
- Ensuring that records retention and disposition schedules are established, authorized as required, and applied to all information in the custody or under the control of a public body.
- A new Transitory Records System (approved in July 2018) was developed to provide public bodies with clearer instruction on the management of transitory records. This schedule is applicable to all Prince Edward Island public bodies defined under the *Archives and Records Act*. A complementary Transitory record guide was published in January 2019.
- Providing a basis for implementing information security measures for sensitive records and for the reasonable protection of personal information.

2.3 DELEGATION OF FOIPP RESPONSIBILITIES

Under **section 72** of the Act, the head of a public body has the power to delegate to any other person any of the head's duties, powers and functions under the Act, except the power to delegate.

A delegation must be in writing and may contain any conditions or restrictions the head of the public body considers appropriate. The delegation instrument should identify the individual to whom the powers are delegated, as well as an alternate individual who will act in their absence.

This type of step delegation ensures that there is someone to whom the delegated functions pass in the absence or incapacity of the primary individual to whom functions are delegated. For example, the delegation instrument should state that certain functions are delegated to A to act generally, and to B in A's absence.

A delegation instrument remains in effect until replaced or until the end of the time period specified in the delegation instrument. If the delegation is to the FOIPP Analyst, the head of the public body may choose to specify that the delegation remains in effect for as long as the individual is employed in the position of FOIPP Analyst.

There is a substantial difference between delegations relating to freedom of information and those relating to protection of privacy.

Freedom of information - delegations relate mostly to the processing of an access request and the decision whether or not to release all or part of a record. The delegation empowers certain officials and employees to make decisions or take action

Privacy Protection – delegations relate to collection, handling and protection of personal information. Delegations are general and center on program areas or local offices that handle the information on a day-to-day basis.

Not every section of the Act dealing with privacy matters calls for delegation of responsibility in a formal sense. The head of a public body should, however, clearly advise managers of their responsibilities, especially with regard to compliance in the collection and disclosure of personal information. In general, delegation should be considered for all provisions of the Act that state that the head of a public body may or must do something.

It is essential when a delegation instrument is put in place that all identified officers or employees know and understand their responsibilities. Job orientation materials should also include a statement about FOIPP responsibilities for each official or employee taking

up a position that includes delegated responsibilities under the Act. The nature of actual delegation is very much determined by the structure of the public body and the approach that it wishes to take toward administration of the FOIPP Act.

The FOIPP Analyst normally prepares the delegation instrument and submits it to the head of the public body for approval.

2.4 LIABILITY, SANCTIONS AND PENALTIES

Protection from Liability

Under **section 74** of the Act, a public body and all the officials involved in the administration of the Act are protected from liability for damages for:

- Disclosing or withholding information, or for the consequences of disclosing or withholding information, where a public official has acted in good faith; or
- Failing to give a required notice where the public official took reasonable care in giving notice.

Section 74.1 protects an employee of a public body from adverse employment action as a result of properly disclosing information in accordance with the Act.

Anyone who violates **section 74.1** is guilty of an offence and liable to a fine of not more than \$10,000.

Offences and Penalties

Section 75 of the Act requires public bodies to cooperate both with the Information and Privacy Commissioner or another person conducting duties of the Commissioner under the Act.

It is an offence to:

- Collect, use or disclose personal information in violation of **Part 2** of the Act;
- Attempt to gain or gain access to personal information in violation of the Act;
- Make a false statement to or mislead or attempt to mislead the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or another person under the Act;
- Obstruct the Commissioner or another person in the performance of the functions of the Commissioner or other person under the Act;
- Fail to comply with an order made by the Commissioner under **section 66**;
- Destroy any records subject to the Act, or direct another person to do so, with the intent to evade a request for access to the records; or

- Alter, falsify or conceal any record, or direct another person to do so, with the intent of evading a request for access under the Act.

Failure to comply with a duty imposed by the legislation or otherwise acting in violation of the Act is not an offence unless it is covered under **section 75(1)**.

The Commissioner may find grounds for believing that an offence under **section 75(1)** has occurred in the course of:

- A review requested by an applicant or other individual under the Act;
- An investigation under **section 50**; or
- A disclosure to the Commissioner under **section 69** regarding possible failure to disclose in the public interest or violation of **Part 2** of the Act.

Any other failure to comply with the legislation that is not an offence under **section 75(1)** is dealt with by the Commissioner under the normal review and complaints process set out in **Part 4** of the Act or in an investigation under **section 50**.

Any person who commits an offence under **section 75(1)** or **section 74.1(1)** is liable, upon conviction, to a fine of up to \$10,000 under **sections 75(2)** and **74.1(2)** respectively.

The Commissioner does not impose the fine. The court would determine whether or not an offence had been committed and impose any fine.

CHAPTER 3

Access to Records

3.1 WHO HAS A RIGHT OF ACCESS

Under **section 6(1)** of the FOIPP Act, any person has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.

There are no restrictions on who may make a request. The applicant can be any person inside or outside Prince Edward Island, including individuals, corporations, and organizations. The Act does not specify a minimum age, which means that minors may make requests.

3.2 RECEIVING A FOIPP REQUEST

Nature of Request

Section 7(1) of the Act provides that an applicant must make a request to a public body that the applicant believes has custody or control of the particular record(s).

Section 7(2) requires that the request be in writing and provide enough detail to enable the public body to identify the record. Applicants may request either to examine the record or to obtain a copy of it (**section 7(3)**). As long as the original request was properly made, a change to the original terms of the request, for example, where the applicant asks to examine records rather than to receive copies, may be verbal.

The initial fee of \$5 must accompany a request for general records. There is no initial fee when the applicant is requesting their own personal information. No tax is charged for FOIPP requests.

Form of Request

The applicant can use the official **Request to Access Information Form, or the on-line submission tool**, or an applicant may simply write a letter, requesting records and referencing the FOIPP Act.

Alternative Forms of Access

Section 4 of the FOIPP Regulations permits applicants to make oral requests if they have:

- A limited ability to read or write English or French; or
- A physical disability or condition that impairs their ability to make a written request may make an oral request.

Public bodies should assist individuals seeking records under the Act who are disabled, do not have literacy skills or are otherwise unable to exercise their rights under regular procedures. This could include:

- Helping visually impaired applicants make a request by filling out a request form.
- Assisting applicants lacking literacy skills by putting their oral request in written form.

Public bodies that are subject to the *French Language Services Act* are required to deal with a request in either English or French, at the option of the applicant.

Where an applicant lives in a remote areas and/or is disadvantaged in comparison with other members of the public in their ability to make a FOIPP request the public body should assist in ways that will enable them to exercise their access rights without excessive cost or delay.

Duty to Assist Applicants

Section 8(1) of the Act requires the head of each public body to make every reasonable effort to assist applicants, and to respond to each applicant openly, accurately and completely.

This duty to assist informs every step of the request process. It is critical during the applicant's initial contact with a public body. The FOIPP Analyst and staff should attempt to develop a working relationship with the applicant to define the nature and scope of the request and determine the steps involved in processing the request. A public body must make every reasonable effort to identify and locate records responsive to a request, and provide the applicant with information regarding the processing of the request in a timely

manner.

Both parties have an interest in the efficient, timely processing of requests. When a FOIPP request can be dealt with outside the Act, a public body should return to the applicant any fees paid and provide copies of the requested record. Procedures for responding to a request outside the Act are discussed in section 3.4 of this chapter.

Identity of the Applicant

A public body should not disclose the identity of the applicant to anyone who does not have a legitimate ‘need to know’. A legitimate need to know relates to the specific knowledge an individual requires in order to process the access request. For example, if the applicant is making an access request for their own personal information then their identity is clearly relevant when searching for records. On the other hand, if the applicant is requesting access to general information, their identity is irrelevant, and no one other than FOIP Analyst would have a need to know their identity.

It is improper to treat applicants differently depending on who they are or what organization they may represent. It would also be improper to broadcast the identity of an applicant throughout a public body or to disclose the identity outside of the organization. This approach is consistent with practices in other provinces.

Acknowledging Receipt of Request

The public body should acknowledge receipt of a request. This acknowledgment may indicate that the request:

- Has been received and processing will commence;
- Is incomplete because the initial fee has not been paid and is required before processing can commence; or
- Is not clear or precise enough and more information is needed to clarify it before processing can commence.

If processing cannot begin immediately, an effort should be made to contact the applicant by telephone to resolve any problems quickly.

A written follow-up to this call is good practice. It will provide a definite reference point as to when processing commenced and a statement of the agreement between the public body and the applicant as to the nature and scope of a request that has been clarified.

Request for the Applicant’s Personal Information

Individuals may also make requests for information about themselves. The same general conditions apply to receiving these requests except that no initial fee is required.

It is usually obvious from the face of the request that someone is requesting their own personal information. In some instances, however, someone else may be applying on behalf of the individual and it will be necessary to determine whether the applicant has the authorization of the individual involved or some other right under the Act. Common examples of persons who might reasonably request information about another individual are the legal representative of the individual, and the parent of a young child.

It may not be clear whether the applicant is requesting their own personal information or general records about a subject in which the individual has been involved. A public body may use the following three-part test:

- Consider the wording of the request.
- Characterize the request as to whether it is primarily for general records or is for personal information about the applicant.
- Decide whether the records relate to and are responsive to the request being made and whether the preponderance of records relates to the individual.

On this basis, the public body decides whether or not it is dealing with a request for personal information. For further guidance on requests by representatives of individuals who may be empowered to seek personal information on behalf of an individual, see Chapter 7.12 of this publication.

Permission to Disregard Requests

In rare instances, a public body may ask the Information and Privacy Commissioner to authorize the public body under **section 52** of the Act to disregard certain requests. The head may be allowed to disregard a request if it is:

- Repetitious or systematic in nature; and
- Processing the request would unreasonably interfere with the operations of the public body, or amount to an abuse of the right to make requests; or
- Frivolous or vexatious.

A request is *repetitious* if it is one in a series of requests by an applicant for substantially the same information or records.

A request is *systematic* in nature if it is part of an extensive pattern of related requests by an applicant or a group of applicants.

A request may be *frivolous or vexatious* if it has no sound basis in fact or is malicious. Public bodies should take into account whether there is a past pattern of conduct that indicates an abuse of the process for access and whether or not the request is made in bad faith or for a purpose other than to obtain access to information.

Examples of requests that might be considered frivolous or vexatious include:

- Continual requests for records that a public body has already established it does not have.
- Requests involving fees made by an applicant who has demonstrated a pattern of abandoning a request whenever a fee waiver is not granted or the Commissioner upholds a fee.
- Requests that show an intention to harass a public body, to “break” the system or to engage in “information warfare”.

The onus is on the public body making a request for authorization to disregard a request under **section 52** to make the case to the Commissioner.

More information on this provision can be found in Chapter 8.9 of this publication.

Clarifying Requests

Vague or overly general requests may increase workloads and lead to review of information that is of little interest to the applicant. Often requests are broad or vague because the applicant lacks knowledge of the public body, its mandate and programs and the type of records available.

The FOIPP Analyst should establish contact with the applicant to better understand what information will satisfy the applicant’s needs. If a request does not sufficiently describe the records sought, a public body should advise the applicant and offer assistance in reformulating the request.

There are several things to keep in mind when seeking to define or clarify a request.

Release of Information Outside FOIPP

It is important to verify whether or not the information needs of the applicant can be satisfied by providing records that are already publicly available or that can be made available through a process of routine disclosure. If this is the case, then the relevant information should be released to the applicant without delay. The applicant should be advised that such information is available without a FOIPP request and that there is no

need to make an application under the Act for similar information in the future.

In some instances, only part of the information can be routinely released. In such cases, this information should be released and the rest of the request processed under the Act.

Narrowing a Request

It is important to discuss with the applicant any request that involves a vast amount of information. An example would be a request for all the records concerning planning in a public body. The objective is to narrow the request while still meeting the applicant's information needs. This can result in a reduction of fees and provision of better service, in terms of both time and results.

Changing the Scope

After discussion of the nature of a request, an applicant will sometimes change the scope of the request. When this occurs, the public body should document the change and send a notice to the applicant.

Time Limits

The Act establishes a time limit of 30 calendar days to respond to a request. The time period begins on the day following receipt of a FOIPP request. A request is complete if it mentions the Act, is signed and includes the initial fee, if required.

As provided in **section 2** of the FOIPP Regulations, the 30-day time period for responding to requests commences on the day after receipt of a request in the office of the public body designated to receive such requests. This office is normally the FOIPP Analyst. The time period begins to run even when the request is vague or imprecise.

Authorized offices are listed on the FOIPP web page on the Government of PEI website and may be publicized in other ways. A request may be delivered to any office of a public body during normal business hours, but the time limit for responding to the request does not commence until the request is received in an office authorized to receive requests.

Time Extension

When an applicant will not narrow or be more precise in a request, or when a request is genuinely broad in nature, **section 12(1)(a)** enables the public body to extend the time for responding to a request for another 30 days (allowing a total processing time of 60 calendar days).

More information is given about extensions of time limits below, under the heading Response Time Limits.

Documenting and Tracking Requests

All public bodies should systematically document deliberations and decisions regarding the processing of requests. This will help ensure that the request process meets the requirements set out in the Act. If the decision is reviewed by the Information and Privacy Commissioner the timeline may also be critical part of the evidence.

Section 2(3) of the FOIPP Regulations requires the public body to have a reasonable system in place to ensure that FOIPP requests are forwarded as soon as possible to the office(s) designated to receive and begin processing them. Reasonable steps might include special forwarding instructions to staff in mail rooms within the public body and to staff that open the mail, as well as use of a color-coded transmittal file to indicate the priority and important nature of the document. Most importantly, staff should be aware of the urgent nature of FOIPP requests and the need to forward them immediately to the FOIPP Analyst. Offices designated to process FOIPP requests should date-stamp all requests on receipt.

Transferring a Request

There are occasions when an applicant makes a request for information to one public body that would be more appropriately handled by another public body. In order to meet the applicant's information needs, it may be better to have the public body that has the greater interest in a record process the request.

Transferring the request to that public body will ensure that people who are familiar with the information are involved in processing the request and that decisions on disclosure are made in the most appropriate context.

Requests for correction of personal information may also be transferred if the information was originally collected, or the record created, by another public body.

The public body originally receiving the request should make every reasonable effort to assist the applicant by identifying the location of the information. This includes ensuring that the public body best able to handle the request receives it.

If the FOIPP Analyst is aware that part of a request relates to records of another public body, the public body receiving the request should inform the applicant that they can make a request to the other organization for the information.

Transfer Procedure

Section 13(1) of the Act provides that within 15 days after receipt of a request a public body may transfer a request, and, if needed, any records relating to it, to another public body if:

- The record was produced by that body;
- The other body was the first to obtain the record; or
- The record is in the custody or under the control of the other public body.

Before a public body transfers a request to another public body, it must ensure that the other public body has a copy of the record and that it agrees to the transfer. A public body may decline to accept a transfer if the requested record has little or no connection to its duties and functions or it believes the receiving body has a greater interest in the record.

Section 34(7) of the Act provides that a public body may transfer a request to correct personal information if:

- The personal information was collected by another public body; or
- Another public body created the record containing the personal information.

This ensures that the public body that originally collected or compiled the personal information makes the corrections, annotation or linkage required. The onus is then on that public body to inform others to whom the information has been disclosed of its decision about the request.

Conditions of Transfer

When a request is transferred, **sections 13(2) and 34(8)** of the Act require:

- The public body that transferred the request to provide notice to the applicant as soon as possible.
- The public body receiving the request to make a reasonable effort to process the request within 30 days after receiving it, unless a time extension is sought under one of the conditions set out in **section 12** of the Act.

The public body to which the request is transferred should also acknowledge receipt of the request.

Requests affecting multiple public bodies

In many cases, interest in the disclosure of particular records will exist in several public bodies. This might be the case, for example, with requests for the records of interdepartmental or multi-organizational committees, or requests for records relating to budgeting processes and programs in which two or more public bodies are involved. For the sake of administrative simplicity and good client service, the public body receiving such a request should process it, consulting and seeking advice from the other interested bodies, rather than attempting to negotiate a complicated sharing of the request. In such cases, the public body processing the request has the final decision as to what will be released.

In the case of multiple requests to several public bodies for similar records, each public body should process the request that it has received, in consultation with the other public bodies through the Access and Privacy Services Office. Access and Privacy Services Office may provide a coordinating function for similar requests directed to a number of provincial public bodies. Such coordination involves explaining difficult issues and promoting communication among public bodies. Decision-making about a request will always remain with the public body processing a request.

Consultation

When a public body receives a request that deals with records that originated in another public body or deals with matters in which another public body has a direct interest, it should consult with that public body. This will ensure that all relevant factors are taken into consideration in deciding whether or not to disclose all or part of the records.

Two public bodies may deal with different aspects of the same matter or policy and may even disagree on policy directions or administrative actions to be taken. The public body receiving the request should ensure that the views of the other body have been taken into consideration in any decision to disclose or to refuse access to all or part of the records concerned.

If more than two public bodies are involved, the consultation process should ensure that all parties are aware of each other's views. Public bodies that regularly need to consult with other public bodies on disclosure in response to access requests may need to set out their procedures for consultation and decision-making in policy.

Response Time Limits

Section 9(1) of the Act provides that public bodies must respond to a request without undue delay and in any event make every reasonable effort to respond to a request no later than 30 calendar days after receiving it, unless:

- The time limit is extended under **section 12**; or
- The request is transferred to another public body under **section 13**.

Every reasonable effort means the effort that a fair and rational person would expect to be made and would find acceptable. A public body's effort is expected to be thorough and comprehensive.

The 30-day time limit is based on calendar days. The time limit begins on the day after the request is received in an office duly authorized to deal with it and any initial fee is paid. If the request is incomplete and further information is required from the applicant in order to identify the records sought, a public body should seek this information immediately. The requirement to clarify the request does not change the date on which the time period commences, but may necessitate a time limit extension.

Deemed Refusal

Section 9(2) of the Act clearly establishes that the failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under **section 12**, can be treated by the applicant as a decision to refuse access to the record(s). Failure to respond to a request may be reviewed by the Commissioner.

Time Limit Extensions

Section 12 of the Act provides authority for extending the time limit for responding to a request. The circumstances in which an extension is permitted are limited and, in some cases, the permission of the Commissioner is required.

A public body may extend the time limit for responding by up to 30 days, allowing a total period of up to 60 days, in the circumstances indicated in below table.

Section 12 (1)(a)	Section 12 (1) (b)	Section 12(1) (c)	Section 12(1)(d)
<p>The application does not contain enough detail to enable the requested records to be identified.</p> <p>The request may be vaguely worded, or for some other reason, the record is impossible to locate from the description provided. Clarification is needed from the applicant.*</p>	<p>A large number of records is requested or must be searched and responding within 30 days would unreasonably interfere with the operations of the public body.</p> <p>This type of request will usually result in discussions with the applicant to try to narrow the scope of the search.</p> <p>This provision does not apply to review of the records in order to make a decision on disclosure but only to the search for and retrieval of the records.*</p>	<p>More time is needed for the public body to consult with other public bodies, other levels of government or third parties.</p> <p>This provision applies to third party consultations as required under section 28 of the Act (which may take up to 20 days), consultation with other governments under section 19 (for which there is no specified time limit), and consultation with other public bodies (where the public body has no legislated power to compel a timely response).*</p>	<p>Allows for a time limit extension when a third party asks the Commissioner to review a head's decision on a request.</p> <p>In order to allow time for the third party to ask the Commissioner to review the decision, an additional 20 days may be required.</p> <p>If a review by the Commissioner is requested by a third party, the information must be withheld until the review is completed and any order issued. *</p>
<p>Section 12(2) also provides for a public body, only with the Commissioner's permission, to extend the time limit for responding to a request in the following circumstances:</p> <ul style="list-style-type: none"> • Multiple concurrent requests are made by the same applicant; or • Two or more applicants who work for the same organization or who work for the same organization or in association with each other make multiple concurrent requests. <p>This provision acknowledges the difficulty that a public body may have if one or more applicants make a number of requests at the same time. It recognizes that the same factors set out in section 12(1) can apply when several requests are made at the same time, even though no single request would present such difficulties.</p> <p>This provision applies to any time limit extension, even if only an additional 30 days is required.*</p>			
<p>Section 12(3) allows the head of a public body to extend the time limit for responding to a request in accordance with individual provisions of the Act, without seeking the permission of the Commissioner, even if the cumulative effect of granting allowed extensions takes the time period beyond 60 days. This may occur if the need to consult with a third party is not recognized until late in the processing of a large request. This provision also protects the rights of third parties to seek a review of any decision to release information about them.</p>			

*When the Commissioner refuses to grant permission for an extension under **section 12(1)** or **(2)**, the public body has a maximum of only 60 days to process the request. Public bodies must continue to process a request while awaiting the Commissioner's response to

an extension request.

The public body should consider all factors relating to the possibility of the need for a time limit extension before finally deciding to invoke one. Common factors include:

- The amount and type of detail required from the applicant to clarify a request.
- The breadth and complexity of the request,
- The number of records requested and the number of files that must be searched to find the requested records.
- The number and complexity of consultations required with external organizations, such as other public bodies or other levels of government.
- The quantity and type of records requiring review by other public bodies. The Act does not regard other public bodies as third parties for the purposes of notices under **sections 28 and 29**. Consultation with other public bodies is therefore not subject to specific time limits, but they should agree to respond as expeditiously as possible.
- The amount of time needed for the Commissioner to deal with a request for review. The Commissioner's office should be consulted on this matter.

The Act does not provide for extensions for other administrative reasons, such as:

- Consultations within the public body after the records have been located.
- Line-by-line review of the records after they have been located.
- Working conditions arising from sickness, staff absence or vacation, or staff workloads.

Limits on Extensions

Public bodies should make every effort to plan the processing of complicated requests so that there is a need to invoke only one extension. A public body may, on its own authority and *within* the original 30-day time limit, extend the 30-day limit for another 30 days or as required to enable the head to comply with requirements of **section 29**.

If the public body believes that responding to the request will require more than a total of 60 days, the head is required to ask the Commissioner for permission to extend the time limit beyond the original 30 days. This must be done in writing and normally within the original 30-day time limit. The reasons for the extension must meet the conditions of **section 12(1)**, as listed above.

For example, if a public body believes that it will take 90 calendar days to process a request, it should request permission from the Commissioner, within the 30-day original

time period, to extend the response time for 60 calendar days (30 original days + 60 day extension = 90 days).

A letter requesting an extension by the Commissioner should set out the specific reasons why a period greater than 60 days is required to process the request. The letter should propose a reasonable period of days for producing a response.

Normally, if a public body has already taken a 30-day extension under its own authority, it should not seek a second extension from the Commissioner. However, this may be done in exceptional circumstances, where complications not originally contemplated when planning the response process arise.

An example might be where a public body has already claimed an extension of 30 days because of the need for extensive consultation. On the 45th day, as a result of that consultation, it discovers additional records that have to be searched and from which responsive records will be retrieved.

In this case, the public body would request the permission of the Information and Privacy Commissioner to extend the period for response to the applicant.

The public body should reference the factors outlined in **section 12(1)** when requesting an extension from the Commissioner. If the Commissioner refuses to grant a time limit extension under **section 12(2)**, the public body may consider each request separately to determine whether an extension is needed.

Documentation

Public bodies must document the reasons for a time limit extension. This is required to support the public body's decision to extend, for a request to the Commissioner for an extension of more than 30 days, and in case of a complaint by the applicant to the Commissioner.

Notification

Section 12(4) of the Act requires a public body to notify the applicant that an extension is being taken, the reason for it, the date when a response can be expected, and that the applicant has the right to make a complaint to the Commissioner about the extension.

This notice is required as soon as it is apparent that the request cannot be processed within the initial 30-day time period.

When a request for extension is made to the Commissioner, the notice should be sent to the applicant before the Commissioner's final decision has been made as to whether or not the extension will be granted. If an applicant complains to the Commissioner about an extension, the public body continues to process the request throughout the review period. After investigating a complaint about a time limit extension, the Commissioner may either confirm or reduce the extension as provided in **section 66(3)(b)**.

Conditions Affecting Response Times

- **Third party notice:** When a public body gives notice to a third party under **section 28**, the deadline for a final response to an applicant must take into account the time required to allow the third party to respond. No decision may be made before *either* 21 days after the day notice is given *or* the day a response is received from the third party, whichever is earlier. The public body should notify the third party as soon as possible after receiving a request in order to minimize the delay in responding.

Giving a third party notice is discussed in Chapter 5 of this publication.

- **Transfer of request:** Where a public body decides to transfer a request to another public body, the Act requires it to do so within 15 days of receiving the request. The second public body then has 30 days after receiving the request to respond, unless it seeks an extension on one of the grounds set out in **section 12**.
- **Day of response:** The Prince Edward Island *Interpretation Act* provides that, if the day a response is due falls on a statutory holiday or a day when the office of a public body required to respond is closed, then the response is due on the next business day.

The head of the public body is responsible for determining whether the office that is authorized to handle requests is closed.

3.3 PROCESSING A FOIPP REQUEST

In general, the FOIPP Analyst will carry out all the duties outlined in this chapter. Public bodies should develop procedures to govern the processing of requests and to ensure that processing occurs within established time limits and in accordance with the requirements of the Act. Public bodies should also create and retain documentation on their processing of requests.

Before beginning to process a request, the FOIPP Analyst should determine whether the request can be handled outside the Act. If so, and if no other fee structure is in place, the

initial fee should be returned to the applicant along with a copy of the records. If there is a procedure in place to refer an applicant to the appropriate program area, the fee should not be returned until the applicant has agreed to have the request handled outside the Act by the program area.

The applicant must agree to withdraw the request; otherwise, the public body is required to respond to it in accordance with the requirements of the Act.

Initial Control

Once a request is received in the office of the FOIPP Analyst, it should be registered and logged (this is done electronically if an automated tracking system is in use).

It should then be placed in a request file and details of the request forwarded to any program area that has custody or control of requested records. The request should be accompanied by an **Access Request Review Form** for recording all activities and the time involved **in searching for records related to the request**, in order to document these activities and assess the appropriate fees.

The identity of the applicant should be disclosed only:

- To those officials and employees of the public body who have a need to know it in order to carry out their job duties.
- To the extent necessary to carry out the public body's functions in processing the applicant's request.

For instance, where the request is for general records, the FOIPP Analyst should forward only the request for records and not the name and other identifiers of the applicant to program areas within the public body.

Locating Records

The program area within the public body is normally responsible for locating and retrieving all records relevant to a request under its custody or control, including those records that may reside in individual employees' offices, vehicles or homes, or in filing systems in storage areas. When applicable, records in the possession of contracted agencies may have to be located.

The program area should draw on the support of records or information management staff in providing the indexes and guides to appropriate records, where these are available, and to locate records.

Speed and accuracy are essential in identifying, locating, retrieving and, where appropriate, copying records pertinent to a request (where a request is for a large number of records, it may be appropriate that copies are not made immediately).

A rule of thumb for a basic, uncomplicated request involving the coordination of staff in different areas is that four working days are needed to pull together the working program file, with the pertinent records that need to be reviewed.

Scope of Search

The Act applies to *all* records, as defined in the legislation, including electronic records, in the custody or under the control of the public body. All types of records responsive to the request, including electronic records, must be located and retrieved.

In addition, all areas where records are held – central active files, working files in individual offices, electronic repositories and off-site storage areas – must be searched, and staff requested to produce relevant records, as dictated by the nature and subject of the request.

Any records in the possession of contracted agencies and under the control of the public body will have to be located, copied, if appropriate, and transferred.

An applicant can ask the Information and Privacy Commissioner to review the adequacy of a search undertaken to locate records. When this happens, the public body will have to demonstrate that it made a reasonable search of all repositories where records relevant to the subject of the request might be located.

“The search must be thorough and comprehensive. Evidence of the search should describe all potential sources of records, identify those searched and identify any sources not searched, with reasons for not doing so. The evidence should also indicate how the searches were done and how much time the public body staff spent searching for records.”

-- Information and Privacy Commissioner of BC, F06-10-MS

“A reasonable search is one in which an experienced employee knowledgeable in the subject matter of the request expends a reasonable effort to locate records which are reasonably related to the request.”

– Information and Privacy Commissioner of Ontario, PO-3172

Conditions Relating to the Disposition of Records

Public bodies must not dispose of any records relating to a request after it is received, even if the records are scheduled for destruction under an approved records retention and disposition schedule.

This includes any e-mail and transitory records relevant to the request that may exist at the time the request is received. In effect, the receipt of a FOIPP request freezes all disposition action relating to records covered by the request until the request has been completed and any appeal to the Commissioner decided.

The file transmitting the request to the program area should include a reminder that it is an offence to destroy any record or direct another person to do so (**section 75(1)(e)**) or to alter, falsify or conceal any record, or direct another person to do so (**section 75(1)(f)**) in order to evade a request for access to records. These offences are punishable by a fine of up to \$10,000.

Where records have been destroyed prior to the receipt of a request, in accordance with an approved records retention and disposition schedule, the public body's response to the applicant should indicate that the records have been destroyed, quoting the authority for and date of destruction.

When records have been transferred to the Public Archives and Records Office or the archives of the public body, the request should be transferred to the archival authority for processing, unless some other arrangement between the two organizations exists.

Copying Retrieved Records

Once the records have been located, either the program area or the office of the FOIPP Analyst, as appropriate, prepares them for review and completes the request documentation.

This may involve the copying and numbering of all records pertinent to the request and preparing:

- A list of all records areas searched.
- A list of the records located in each records area, along with identifying data and parts of file lists, data dictionaries or other finding aids used in locating the records.
- A log of staff time spent searching for and retrieving the records.

When there is a very large number of records involved, lists of the records rather than copies of them may be more appropriate.

Preliminary Assessment

There are a number of administrative matters that the FOIPP Analyst should consider very early in the request process, but after the program area has had an opportunity to consider the extent and nature of the request and to locate the records. This discussion will inform the preliminary review of the records, which will be done either by the FOIPP Analyst or, in larger organizations, by the FOIPP Analyst in cooperation with the program contact and representatives knowledgeable about the subject matter and records involved.

Questions to ask at this stage are:

- Does it appear that all relevant records have been located and do they appear to satisfy the request?
- Are there any records referenced in the request or the located records that have not yet been located?
- Are any of the records excluded from the scope of the Act under **section 4** or subject to other legislation that prevails over the FOIPP Act?
- Can the records, in whole or in part, be released immediately without line-by-line review?
- Should all or a portion of the request be transferred to another public body with greater interest in the records? See **section 3.2** of this chapter, Response Time Limits, for legislative requirements and policies relating to the transfer of requests.
- Does it appear that records may be found in program areas other than those already identified, and should the search be widened?
- What is the extent and nature of consultation required with other program areas within the public body? Responsibility for ensuring that these consultations occur should be clearly assigned.
- What is the extent and nature of external consultation required with other public bodies and levels of government? Responsibility for conducting these consultations should also be clearly assigned.
- Do the records contain third party business information or personal information that may require third party notification?
- Will the time required to respond to the request likely exceed the 30-day time limit? Are there grounds for an extension of the time limit?
- Will fees in addition to the initial fee (if applicable) be assessed for the processing of the request?

From this preliminary review, the FOIPP Analyst may, depending on the level of delegation, either recommend or undertake actions related to:

- The transfer of all or part of the request;
- The immediate release of all or some of records;
- The extension of time limits;
- Third party notification; or
- The assessment of fees.

Each of these activities involves a notice to the applicant. Notices are considered in this publication as follows:

- Release of a record is discussed in **section 3.4** of this chapter.
- Extension of time limits is discussed in the **section 3.2** of this chapter, Response Time Limits.
- Third party notification is discussed in Chapter 5.
- Transfer of requests is discussed in **section 3.2** of this chapter.
- Fees are discussed in this **section (3.3)** below.

Notices

Various notices are required under the Act. Of particular importance are notices which:

- Inform an applicant of a fee estimate.
- Report to an applicant about the progress of a request (e.g., any extension of the time limit for responding).
- Notify a third party (a business or an individual) that information provided by the third party or personal information about the third party has been requested, and that an opportunity is being provided for comment as to whether or not the information should be disclosed.
- Advise the applicant of the decision on the disclosure and provide information about access to the requested records if access is granted.

Section 70 of the Act provides that a notice or other document to be given to a person is to be given:

- By sending the notice or document by prepaid mail to the last known address of the person;
- By personal service;
- By substituted service if authorized by the Commissioner; or
- By means of a machine or device that electronically transmits a copy of a

document, picture, or other printed material by means of a telecommunications system.

The choice of how to give notice or send a document depends on the circumstances. Normal methods will be by mail, fax **or if appropriate email**, since these are common, effective ways of communicating. There will be circumstances, however, when other methods may have to be used. This may be the case when addresses are uncertain, when the number of persons, organizations or groups to be contacted is large, or when there is a need to assure delivery to a specific person.

Personal service means a method of delivery whereby it can be shown that the person to be served actually received the document.

Substituted service usually takes the form of a notice presented in the media. This may be a general notice, as often appears in newspapers and weekly journals, or a more specific notice (e.g., a third party notice to a large number of small companies) published in the leading trade magazines for the particular business sector concerned. Public bodies should assess the circumstances requiring the notice and choose the most effective and economical approach.

Assessing Fees

An important principle underlying the FOIPP Act is the use of fees to help offset the cost of providing applicants with access to records under the legislation. The Act provides for a reasonable and fair fee structure that is intended to support effective provision of FOIPP services.

Section 76 establishes that:

- A public body may require an applicant to pay fees for services as provided for in the FOIPP Regulations (**section 76(1)**).
- For personal information, such fees shall be restricted to the cost of providing a copy of the information (**section 76(2)**).
- If fees are required under **section 76(1)**, an estimate of the total fee must be prepared by the public body for the applicant before providing the services (**section 76(3)**).
- Applicant may, in writing, request the head to waive part or all fees for service (**section 76(3.1)**).
- The public body, or the Commissioner if requested, may excuse an applicant from paying all or part of a fee if, in the opinion of the head of the public body or the Commissioner, as the case may be:

- The applicant cannot afford the payment or for any other reason it is fair to excuse the payment; or
 - The record relates to a matter of public interest, including the environment or public health or safety (**section 76(4)**).
- The fees referred to in **section 76(1)** must not exceed the actual costs of the services provided.

Taxes are not charged on fees for processing FOIPP requests.

General Records

Section 9 and **Schedule 2** of the FOIPP Regulations set out the fees that may be charged for processing a general access request.

The head of a public body may require an applicant who makes a request under the Act to pay fees for the following services:

- Locating and retrieving a record;
- Producing a record from an electronic record;
- Preparing a record for disclosure (to cover the time taken to physically sever the record);
- Providing a copy of a record;
- Creating a new record under **section 8** of the Act; and
- Supervising the examination of an original record.

No fee may be assessed for time spent in reviewing a record to determine whether or not all or part of it should be disclosed. If new records have to be created from an electronic record, the public body may use acceptable industry standards to ensure accuracy and completeness of the records, process the information according to its usual procedures, and charge for these services as a part of its fee. The fee provision is discretionary in nature, but normally fees will be assessed for all general requests under the Act. Fee waiver provisions are set out in **section 76(4)** of the Act. The FOIPP Regulations set out the schedule of maximum fees that may be charged. Public bodies may choose to charge less than these rates but not more.

A person who makes a request for access to a general record, which is not a record of the applicant's own personal information, is required to pay an initial fee of \$5.00 at the time the request is made. This initial fee covers the work involved in registering the request, locating and retrieving records, and in some instances providing access to records. For

simple, straightforward requests involving a small volume of records, it will be the only fee paid. For complex requests or requests involving a large volume of records, the initial fee would probably not cover location and retrieval of all records, but would cover the preparation of a fee estimate.

No additional fees are charged unless the amount of time required to process the request for general records, as calculated by the public body to which the request has been made, exceeds **three** hours. The maximum fees to be charged for services provided to applicants are set out in **Schedule 2** of the FOIPP Regulations.

Processing of a FOIPP request for general records must not commence until the initial fee has been paid.

Fee Estimates

Section 11 of the FOIPP Regulations governs the provision of fee estimates under the Act.

When an estimate is provided to an applicant in accordance with **section 76(3)** of the Act, the applicant must be provided with the following details:

- The time required and cost of locating and retrieving the record.
- The time required and cost of preparing the record for disclosure.
- The cost of copying the record.
- The cost of any computer time involved in locating and copying a record or re-programming to create a new record, as appropriate.
- Supervision costs when an applicant wishes to examine the original record.
- Any costs for shipping records to another location for examination or for shipping copies of records directly to the applicant.

This detailed estimate is provided to the applicant as a part of a notice that includes:

- A request that at least 50% of the estimate be paid in advance of the request being processed.

- A proposed agreement for the payment of the fee which, if satisfactory to the applicant, must be signed by the applicant and returned to the public body.
- A statement that the applicant has 20 days to inform the public body that the estimate is accepted and to pay the deposit.
- A statement that the applicant has the right to ask the head of the public body to excuse all or part of the fee and may request a review by the Information and Privacy Commissioner if the fees are considered too high or otherwise inappropriate, or if a request for a fee waiver has not been granted.

This information gives the applicant the basis on which to accept the charges or take other action. This might include narrowing the request, reviewing original records, which would incur supervision costs but would cut down on copying costs, seeking a fee waiver, or requesting review of the fees by the Commissioner under **section 60(1)** or **section 50(2)**.

No further processing takes place until one of the following events occurs:

- The authorized office receives a letter from the applicant agreeing to the charges and attaching payment of the deposit;
- The authorize office receives written notification modifying the applicant's request, and establishing a new basis for assessment of fees;
- The public body agrees to a request for a fee waiver; or
- The Commissioner carries out a review and decides whether the fees are appropriate or the head of the public body has appropriately exercised his or her discretion regarding a request for a waiver of fees, as applicable.

An applicant has up to 20 days to indicate whether or not the fee estimate is accepted. The applicant may modify the request so as to change the amount of fees assessed. If no response has been received after 30 days, the public body may declare the request to be abandoned (see later in this section).

Fee estimates are not binding. However, a public body should do its best to estimate what the fees will be. The public body can revise its estimate in the course of processing the request, and may do so in cases where, for example, records are poorly organized.

If the estimate is too high, provision is made for making a refund to the applicant. If a fee estimate is too low, the public body has the discretion to request additional fees from an applicant. However, the fact that fees will be higher must be addressed with an applicant as soon as it becomes apparent and not be left to the end of the processing period.

Two Minute Rule to Calculate Time to Prepare and Handle Records

In Order No. 03-001 (May 21, 2003), the OIPC wrote that two minutes per page is the

guideline used to calculate preparation time.

The OIPC agreed with the public body that two minutes per page is a reasonable preparation time for making severances to records, where only a few severances per page are being made.

In Order 03-001, the Commissioner wrote that “in most cases, not all pages will be severed. Therefore, it is incumbent upon the Public Body to provide an estimate as to the number of pages to be severed. This will be a difficult estimate to make in the beginning as our Act is new and the Public Bodies are not accustomed to making quick assessments of exceptions under the Act. However, over time, this will become much easier for the Public Bodies. Keeping in mind that a predominant purpose of the Act is to provide access to records, the public bodies should estimate conservatively, in favour of the Applicant who is seeking access.”

The OIPC also wrote “... the fee estimate is only an estimate and if the actual cost turns out, in reality, to be higher, the Public Body can notify the Applicant of the rising costs and the parties can then work out a solution.”

Personal Information

Section 10 of the FOIPP Regulations establishes fees to be charged to an individual for accessing their own personal information. In the case of a request for an applicant’s own personal information, an applicant will pay only copying fees either actual or estimated.

Deposits and Payment of Fees

Processing of a request ceases once a notice of estimate has been forwarded to an applicant and recommences immediately upon:

- Receipt of an agreement to pay the fee; and
- Receipt of at least 50% of the estimated fee

The balance of any fee owing is payable at the time the records are provided to the applicant (FOIPP Regulations, **section 12(2)**).

If the amount paid is higher than the actual fees required to be paid, the balance paid will be refunded (FOIPP Regulations, **section 12(3)**).

The applicant should not be provided with access to a record until all fees owing for the processing of the request have been paid (**section 6(3)** of the Act).

Waiving Fees

Section 76(4) provides that a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the public body:

- The applicant cannot afford the payment or for any other reason it is appropriate to excuse payment; or
- The record relates to the matter of public interest, including the environment or public health or safety.

Normally, an applicant will take the initiative in requesting a fee waiver, usually at the time of submitting the request itself. A public body must consider the request for a fee waiver from an applicant at the time it is made. Fee waiver requests may be made as part of the FOIPP request or after the applicant receives the fee estimate.

The public body does not need to waive all fees if it decides to grant a request to excuse payment. It can consider reducing the fee by a part of its total or not charging for certain services.

If an applicant has requested a fee waiver, and the public body does not grant it, the public body must notify the applicant that they may ask the Commissioner for a review of this decision (**section 76(4.1)**).

The Commissioner may conduct a review of the decision by the head of the public body under **section 60(1)**.

Section 76(4) establishes the criteria for excusing payment of all or part of a fee.

Applicant Cannot Afford to Pay

In very limited circumstances, applicants may be indigent or living on social benefits but require information to assist them in exercising individual or group rights. This type of situation arises most frequently with requests from individuals for information about themselves. Normally, applicants will state in a request why they are seeking a waiver. If they do not or if more information is required, the FOIPP Analyst should phone the applicant and seek the information needed to make a decision.

Applicants should not have to undergo a wealth test to qualify for this type of waiver, but basic information on income and situation should be sought to satisfy the public body that an applicant may fall into this category. For instance, applicants may be asked to show evidence that they would suffer hardship if they were obliged to pay the required fee,

including general information about their sources of income.

Other Reasons Why It Is Fair to Excuse Payment

The head of a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the head, it is fair to excuse the payment for any reason other than financial hardship.

Commissioner's Orders have established that the onus is on the applicant to provide the reason why it is fair to excuse payment (*PEI OIPC Orders 07-004, 08-001*). In some cases, the Commissioner has granted a fee waiver on grounds of fairness where the applicants requested a waiver on other grounds (*Alberta IPC Orders 96-022, 99-027 and 2001-042*).

Section 76(4) may also be used by a public body when it wishes to grant a fee waiver on its own initiative.

The reasons to excuse fees on grounds of fairness may relate to any number of matters. The following are some examples of circumstances where the fees may be waived on grounds of fairness.

- **The public body has assessed fees where the records provide little or no information (see *Alberta IPC Order 99-027*).**
- **The public body has failed in its duties in processing the access request (e.g. by conducting an inadequate search for records or allowing undue delay; see *Alberta IPC Orders 99-039, F2003-023*).**
- **More than one applicant made the same or a similar request at around the same time, and it would not be fair for the public body to collect the total estimated amount of fees from both applicants or to charge the first applicant substantially more than the second (see *Adjudication Order 2*). Alternatively, previous applicants have been given similar records at no cost (see *Alberta IPC Order F2006-032*).**
- **The information requested is important to bring closure to issues and concerns that have been outstanding between the public body and the applicant for a long time (*Alberta IPC Orders 2001-042 and F2007-023*).**

Other factors may also be relevant in deciding that fees should be waived on grounds of fairness such as the following.

- **The records are critical for the applicant to exercise their rights, or are directly related to an individual's personal financial or health management.**
- **A person has a legitimate reason to request the personal information of**

another individual, but cannot exercise that individual's rights under section 76(2) (if that individual requested the information, the request would be subject to copying fees only).

Waiver of the fee would not significantly interfere with the operations of the public body, including other programs of the public body (*Alberta IPC Order F2006-032*).

- **There are no less expensive sources of the information (*Alberta IPC Order F2006-032*).**
- **The request has been made as narrow in scope as possible and the public body has helped the applicant to define its request (*Alberta IPC Order F2006-032*).**

The Alberta Commissioner has declined to waive fees where the applicant was in a position to reduce the fee, by not seeking access to records already provided in response to a previous request, and had not done so (*Alberta IPC Order 99-027*).

Some examples of situations where it might be fair to excuse payment are:

- An individual seeking their own personal information shows that the information is vital to the exercise of their rights.
- The information is of general interest to several applicants and the records are being released to them more or less simultaneously. The first applicant should not bear the total processing costs for all the others and fees may be reduced accordingly.
- The information requested is important to bring closure to issues and concerns that have been outstanding between the public body and the applicant for a long time (*IPC Orders 2001-042 and F2007-023*).
- Other factors may also be relevant in deciding that fees should be waived on grounds of fairness such as the following.
 - The records are critical for the applicant to exercise their rights, or are directly related to an individual's personal financial or health management.
 - A person has a legitimate reason to request the personal information of another individual, but cannot exercise that individual's rights under **section 6** (if that individual requested the information, the request would be subject to copying fees only).

Record Relates to a Matter of Public Interest Section 76(4)(b)

The head of a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the head, the record relates to a matter of public interest, including the environment or public health or safety.

The concept of public interest has been explained in a number of Commissioner's Orders in both Alberta and Prince Edward Island. (PEI OIPC Orders FI-11-002, 08-001). The term "public" may be applied to *everyone* and *anyone*. The term "interest" can range between the sense of individual curiosity and the notion of interest as a benefit. The Commissioner has reasoned that the weight of public interest depends on a balancing of the relative weight afforded to curiosity and benefit, and to a broad versus a narrow public. The Commissioner has also said that public interest is not confined to environmental and public health and safety issues. This category of fee waiver is appropriate when the information is likely to contribute significantly to public understanding of the operations or activities of the public body, or is of major interest to the public.

It should be noted that the criteria for determining public interest under **section 76** are not the same as for the Act's provision for disclosure in the public interest (**section 30(1)(b)**). **Section 30(1)(b)** overrides all other provisions of the Act, including its provisions for the protection of personal privacy. Public interest in **section 30(1)(b)** must be narrowly interpreted, limited to compelling public interest. **Section 76(4)(b)**, on the other hand, is intended to support access rights, and is therefore interpreted more liberally. (See Alberta *IPC Orders 98-011, 98-019 and 2000-031*.)

There are two overriding statutory principles that must be taken into account on a general basis when dealing with both FOIPP fees and fee waivers:

- The Act is intended to foster open and transparent government, subject to the limits contained in the legislation.
- The Act contains the principle that the user should pay.

PEI's OIPC Order 03-001 sets out the factors a public body should consider when making a decision on a fee waiver request, and the following 2-step analysis:

- (1) Does the record relate to a matter of public interest?**
- (2) and, if so, should the fees be waived?**

Order FI-11-002 expands on the first step of the above noted test, suggesting at paragraph [73] the following guiding questions to help determine whether records can be considered records of public interest:

- 1. Will the records contribute to the public understanding of, or debate on, or resolution of a matter or issue that is of concern to the public or sector of the public, or that would be if the public knew about it? The following factors may be relevant:**
 - **Have others besides the applicant sought or expressed an interest in the records?**
 - **Are there other indicators that the public has or would have an interest in the records?**

2. **If the records are about the process or functioning of government, will they contribute to open, transparent and accountable government? The following factors may be relevant:**
- **Do the records contain information that will show how the Government of PEI or a public body reach or will reach a decision?**
 - **Are the records desirable for the purpose of subjecting the activities of the Government of PEI or a public body to scrutiny?**
 - **Will the records shed light on an activity of the Government of PEI or a public body that has been called into question?**

Public bodies should consider these questions when exercising their discretion as to whether to waive or reduce fees. A public body may ask an applicant requesting a fee waiver in the public interest to provide information relating to any of the points that appear relevant to the records under consideration.

If the Commissioner conducts a review of a decision not to grant a fee waiver in the public interest, the public body may find it helpful to show that it considered these points in making its assessment.

Abandonment of Requests

Often, it is clear when an applicant has decided not to pursue a FOIPP request. Applicants will indicate either in writing or on the telephone an intention not to proceed with the request. This may be for a variety of reasons – for example, they have found that the information is available to them outside the FOIPP process or they no longer need the information.

Sometimes, situations will arise where an applicant simply ceases to respond during the processing of a FOIPP request. No indication is given that the applicant has decided not to pursue the request. They simply do not respond to queries from the public body.

When this latter situation occurs, **section 7 (4)** of the Act sets out provisions for declaring a request to be abandoned. The public body must have contacted the applicant in writing, and either sought further information that is necessary to process the request, or requested payment of or agreement to a fee.

If the applicant does not respond within 30 days of being contacted, the public body can advise the applicant, again in writing, that the request has been declared abandoned. A specific date for this declaration should be included in the notice. This notice must state that the applicant can ask for a review by the Commissioner of the decision. In most cases, abandonment of a request occurs before processing of the request is completed. However,

in some cases, an applicant abandons a request after processing is completed.

If the public body has responded to the applicant's request, stating where, when and how access will be given; and has requested that the applicant contact the public body about viewing the records; and the applicant does not respond within 30 days, then the public body can advise the applicant that the request has been declared abandoned. The procedure outlined above will apply to such requests. It is good practice for a public body to keep the file active for a further 60 days in order to allow time for the applicant to request a review by the Commissioner.

Responsive Information

Records that have been identified as responsive to a request in an initial search may include information that is not responsive. Careful examination of the request is required to ensure that the reply is complete but also that information that is non-responsive to the request is removed.

The fact that an applicant already has or knows the substance of the information, or has knowledge of the contents of the record, does not mean that the record can be considered non-responsive. The public body's obligation is to address the applicant's entire request. However, a public body and an applicant may agree not to make copies of records available in order to save costs.

Removal of non-responsive information must occur before severing takes place using the exceptions in the Act. This process applies only when an applicant requests specific *information*, such as their own personal information. If an applicant asks for a *record*, then the whole record is generally considered responsive and any part of the record that is not to be disclosed must be severed on the basis of the exceptions in the Act. Despite this general rule, the public body may treat portions of a record as non-responsive if they are clearly separate and distinct and entirely unrelated to the access request.

Certain records that are identified as responsive to a request may be records that are excluded from the scope of the Act under **section 4**. If a public body chooses to provide access to excluded records, it should be made clear to the applicant that the records are outside the scope of the Act. For information responding to a request involving excluded records, see **section 3.4** of this chapter.

Line-by-Line Review of Records

Once the preliminary assessment has been completed, the various administrative matters have been sorted out and any necessary consultations are under way the FOIPP Analyst will need to review the documents line by line.

A line-by-line review is essential to comply with the principle of severability set out in **section 6(2)** of the Act. This provision grants an applicant a right of access to any record from which excepted material can be reasonably severed.

Chapter 4 of this publication deals with the guidelines for the application of the exceptions to the right of access. The reviewer offers a perspective on any harm that may result from release of particular information and identifies factors to be taken into consideration when exercising discretion to release or refuse access to the information. During a line-by-line review, the FOIPP Analyst may identify additional requirements with respect to third party notices or consultations.

Documentation

During the line-by-line review, the person who reviews the records should document exceptions to be invoked, actions to be taken, reasons for each decision, and recommendations for responding to the request.

Public bodies should complete the Access Request Review Form to provide a detailed record of the results of the search, and concerns related to disclosure of records. This will guide the FOIPP Analyst on how, when to apply exceptions.

Thorough documentation at this stage ensures that the public body has the information required to assess recommendations from the program area and to formulate final decisions relatively quickly. It minimizes duplication of effort and ensures that the public body is in a position to explain decisions both to the applicant and to the Commissioner's Office, if there is a request for a review.

Reviewer's Recommendations

The person who reviews the records generally should prepare a summary of recommendations that identifies:

- Information recommended for release.
- Specific records or parts of records that are excluded from the scope of the Act.
- Specific records or parts of records to which mandatory or discretionary exceptions to disclosure apply, with the reviewer's recommendations and reasons with respect to the discretionary exceptions (for guidance on the exercise of discretion, see Chapter 4 of this publication).
- Other general factors that may be pertinent in reaching a decision on a response to the request.

This report forms the basis for a discussion between the FOIPP Analyst and the program area of recommendations for a draft final report on the response.

At this stage any legal advice needed to resolve issues arising from the request should be sought. Similarly, any interpretative or policy issues which need to be raised should be identified and consultation undertaken.

The draft final report should contain:

- A log of staff time spent locating, retrieving, copying and reviewing the records.
- A summary of file systems, offices and records storage facilities searched.
- Copies of records covered by the request (where this is possible and appropriate given the volume of records or the fact that the applicant wishes to view the original records).
- Documentation of the line-by-line review, identifying the specific information in the retrieved records that it is proposed to exempt from access.
- A summary of third party notices sent and responses received.
- Summary of results of consultations with other public bodies and levels of government.
- A written summary of recommendations for release or refusal, including brief background information to explain decisions.

Creating a New Record

Under **section 8(2)** of the Act a public body has the obligation to create a new record from an existing electronic record if:

- The record is in the custody or under the control of the public body.
- The new record can be created using the public body's normal computer hardware and software and technical expertise.
- Creating the record would not unreasonably interfere with the operations of the public body.

The creation of a new record is part of the public body's duty to assist the applicant in locating the information that is the most useful and responsive to their request. The creation of a new record from data that can be manipulated may be an advantage to public bodies in some instances.

Excepted material can sometimes be easily suppressed, saving long and tedious severing procedures. The applicant is also often very satisfied with the information they receive because it is in a more usable or understandable form. This provision is one to consider when dealing with requests involving electronic data and information. This is the only case where the legislation requires a public body to create a new record.

Care should be taken to explain the methods used and what information is being suppressed so that the applicant does not think that information is being manipulated to alter the record

or place a different perspective on it. Public bodies should also take reasonable steps to ensure the information is accurate.

This provision is mandatory but extends only to situations where the record can be created using the normal hardware, software and technical resources of the public body, and when creating the record would not unreasonably interfere with the operations of the public body.

The FOIPP Analyst should consult with both the program and information technology areas to assess the time and resources that would be required to create the record and the impact that this use of resources would have on its day-to-day activities.

A public body may also decide to create a record, even when there is no requirement to do so, if an applicant requests information to which a discretionary exception applies and the public body is willing to disclose the requested information but not the record containing the information.

Severing Information

Many records contain both information that can be released and other information that should be protected from disclosure. When information that falls within an exception can reasonably be severed from a record, an applicant has a right of access to the remainder of the record (**section 6(1)**).

When a discretionary exception applies, a public body must use discretion not only in applying the exception, but also in determining how much of the information is severed. This is the reason for undertaking a line-by-line review of a record. The object of severing is the use of discretion to release as much information as possible, without causing the harm contemplated by the exception.

The only exception to this procedure is when using the exception for legal privilege. When legal privilege applies to a record, the whole record is protected.

Scope

Severing applies to all records regardless of format or previous actions taken. The fact that an applicant may already have obtained copies of some of the records in other ways does not preclude severing to respond to a request.

When severing is required for information stored on specialized media, technical expertise should be sought as to the best way to excise information while recording that severing has been done and for what reason.

In some rare cases a record cannot be severed. The public body then refuses access to the whole record and must be prepared to demonstrate to the Information and Privacy Commissioner the technical reasons underlying the inability to sever. Examples include

personal information of two or more individuals so intertwined in a record that severing would be extremely difficult and time-consuming, or when, after severing, the severed record would make no sense.

Procedures

During the line-by-line review of records pertinent to a request, the reviewer should mark up copies of paper-based records and keep notes about information in other media that may qualify for an exception. The review and severing of records may require a significant amount of time. The review procedure should ensure that all records responsive to the request are reviewed.

The objective in severing is to remove from the body of a record only the information that meets the conditions for an exception. The Act requires that all information in a record that is responsive to the request and which will be intelligible to the applicant after severing be disclosed.

The process is governed by reasonableness, and the public body exercises discretion in determining whether or not discrete portions of information contribute to the overall understanding of the subject matter at issue.

Employees should be encouraged to draft documents with information that the public body may wish to protect, such as recommendations and advice or personal information, segregated in particular parts of the document. This will make the severing process more efficient for current and future documents.

Part of the final decision as to what information will be released and what information will be refused is also a decision on the extent to which the severing process will be applied. Once that decision is taken, the FOIPP Analyst should ensure the excepted portion of a copy of the record is not decipherable and recopy it to obtain the record to be released.

The FOIPP Analyst must ensure that none of the excepted information remains visible.

Indication of Severing

Regardless of the severing method, a public body must indicate the section number of any exception used to sever information, either in the space left after the severing or in the margin closest to the severed information. Where one or more entire pages have been removed, the number of pages severed must be indicated, along with an explanation of the applicable exception(s) used to sever the information.

In cases where a single page or a continuous sequence of pages has been totally severed, the exception(s) applied and the pages to which they applied should be listed in the response letter or collated on a single page. It is neither necessary nor helpful to provide

applicants with multiple blank pages.

In some cases, particularly with law enforcement records, placing the relevant section in the space of the severed information may itself reveal or imply information that could cause harm. The inclusion of the reason for an exception with the remainder of the record could result in an indirect form of information disclosure. In these circumstances, it is permissible for the public body to omit section numbers on the severed pages and list the relevant sections supporting severance in the letter of notification.

Indicating why information was severed from records helps an applicant understand why part of the information requested has been refused and permits an independent review of the decisions taken by the public body.

Maintenance of Copies

A public body should keep a file for each request processed. This file should include an unmarked copy of the records gathered in response to a request and a copy of the severed documents released to the applicant.

This practice helps support the public body in any review by the Information and Privacy Commissioner, and in making decisions regarding requests for the same or similar records in the future.

Maintaining copies can simplify the process of responding to the same or a similar request. However, unless the new request is made shortly after the original, there is still a need to review the records again. The passage of time and any changes in the context surrounding the records may result in more information being released. The rule is that each FOIPP request needs to be processed as a separate request and decisions need to be made in relation to the particular circumstances that apply at the time of the request.

This does not mean that every request is unique. There are similar types of requests that lend themselves to categorization and simple release mechanisms. Often it is possible to create easily severed documentation that is released routinely. This might be done either because the information is in high demand or because disclosure of the information supports overall accountability for a program or activity. In some cases, pro-active dissemination may also be warranted.

3.4 RESPONDING TO A FOIPP REQUEST

Section 10(1) of the Act provides that an applicant must be told:

- Whether access to the requested record or part of it is granted or refused.
- If access is to be granted to the record or part of it, where, when and how access

will be given.

- If access is to be refused, the reason for refusal and the provision of the Act on which this is based, the name and location of an employee who can explain the reasons for the refusal, and that the applicant may ask for a review of that decision by the Information and Privacy Commissioner or an adjudicator, as the case maybe.

When providing an applicant with access to his or her own personal information, a public body must be satisfied that the individual receiving the information is, indeed, the individual the information is about or a duly appointed representative of that person.

For information on appointment of representatives see Chapter 7.12 of this publication.

Identification can usually be confirmed from the context of the request process, but, where there is doubt or the information is sensitive, the public body should request normal identification (ex. a birth certificate or driver's licence) before providing the information.

Fees

In responding to applicants, public bodies must collect all outstanding fees before releasing the records to the applicant.

See Chapter 3.3 of this publication for information on assessment of fees.

Model Responses

The applicant must be provided with a response to a request. In all cases when access is denied, where the record is excluded from the Act, or where the public body refuses to confirm or deny the existence of a record, the response letter must state that, if the applicant requests a review of the decision by the Information and Privacy Commissioner, they should provide the Commissioner with the request number assigned by the public body, a copy of the decision letter, and a copy of the original request when requesting a review.

Generally, the response letter should address the outcomes of the search and review of records in response to a request.

Record Does Not Exist

The public body cannot locate records responsive to the request. If, after consulting with the applicant, it still appears that no records exist, a letter should be sent informing the applicant of that fact and of the steps taken to attempt to find records. Where a record has been destroyed prior to receipt of the request, information should be provided on the date of destruction and the authority for carrying it out (ex., the appropriate records disposition number or authorization).

Access Is Provided

There is a determination that access will be provided because the information falls within the scope of the Act, and the information does not qualify for any exception, or it qualifies for a discretionary exception but the public body has used its discretion in favour of releasing the information.

Some requests will involve records that take little time to review or are easily releasable. In these instances, the public body should release available records as soon as possible rather than waiting until all records are ready for disclosure. This is often possible when some records are ready for release and other records have been sent to third parties for consultation. The applicant will have indicated, in accordance with **section 7(3)** of the Act, whether they wish to receive a copy of the record or to examine the original record.

If the request is for a copy and it can be reasonably reproduced, **section 11(2)** of the Act requires that the copy be included in the package. This will be done only if the balance of the fees has been paid.

If it is not possible to include the records, the same provision requires that the applicant be given the reason for the delay and told where, when and how the copy will be provided. Delay at this stage is unusual, except where there is a requirement to pay any outstanding fees before access is provided. In some instances, the applicant may have asked to examine a record but the record cannot be reasonably severed for examination or the record is in a format that does not readily lend itself to examination (e.g., a microfilm with much excepted material on it). In these instance, the public body may choose to provide a copy of the record to the applicant. **Section 3** of the FOIPP Regulations covers the two types of situations described above.

Excluded Records

In some instances all or some of the records may be excluded from the scope of the Act under **section 4**. Where this is the case, the applicant is informed that the record or information is excluded from the application of the Act. The letter should cite the specific exclusion in **section 4** that applies, and state that the applicant has the right to ask the Information and Privacy Commissioner to review the decision of the public body that the specified exclusion in **section 4** of the Act applies.

It may occur that a record responsive to a request is excluded from the application of the Act, but the public body is considering providing access to it outside the Act. In such cases, public bodies should consult with any affected parties. For example, if the record was created by or for an Officer of the Legislature or an MLA, the Officer of the Legislature or the MLA concerned should be consulted.

In instances where access is provided to an excluded record, it is important that the letter of response inform the applicant that the record is excluded, citing the provision of **section 4** that applies, but indicating that the public body has chosen to provide access to the record outside the Act.

Access Denied

Access is denied to all or part of a record if the information falls within a mandatory exception; the information falls within a discretionary exception and the decision is to deny access; or the information lies outside the scope of the Act. In these instances, the response provides:

- The reasons for refusal and the sections (i.e., the specific subsections and paragraphs) on which the refusal is based.
- The name, title, business address and business telephone number of the FOIPP Analyst or other official who will answer any questions the applicant may have.
- A statement that the applicant has the right to request a review of the decision under **section 60(1)** of the Act and that this request must be made within 60 days after notification of the decision.

Refusal to Confirm or Deny Existence of Record

In some circumstances, the knowledge that a record exists may cause harm to a law enforcement matter (**section 18**), may pose a danger to an individual's or the public's safety (**section 16**) or may invade the personal privacy of a third party (**section 15**).

Section 10(2) of the Act permits a public body to refuse to confirm or deny the existence of a record in these instances.

Copies of Requests and Records

When a public body has responded to the applicant, the FOIPP Analyst should ensure that the request file is complete and includes:

- All internal and external correspondence.
- Copies of records reviewed.
- Copies of all records that were released to the applicant, either severed or complete.
- Any other information documenting the request management process.

Closure and Retention of Request Files

It is good practice to keep a request file active for 60 days after responding to a request in order to allow time for a request for a review by the Commissioner. If a review is

requested, the file will be reopened and remain open until the review process is complete.

Once the file is closed, either because the public body has responded to the request, or a review has been completed, the public body must retain the file for at least one year to meet the retention requirements of **section 33(b)** of the Act. Unless a shorter time is agreed to in writing by the individual, the public body or the body that approves the records retention and disposition schedule, if different from the public body. Section 33 (b) was amended in 2018 as follows:

- (b) retain the personal information for
 - (i) the period required by the records retention and disposition schedule for the public body, as required by the Archives and Records Act or another enactment that applies with respect to that public body, or
 - (ii) if subclause (i) does not apply with respect to the public body, at least one year after using it.

In addition to meeting the requirements of the FOIPP Act, a public body is also obliged to comply with its records retention and disposition schedule.

CHAPTER 4

Exceptions to the Right of Access

4.1 OVERVIEW

Section 2(a) of the FOIPP Act allows any person a right of access to records in the custody or under the control of a public body. **Section 2(c)** allows individuals a right of access to personal information about themselves that is in the custody or under the control of a public body.

Both rights are subject to limited and specific exceptions where release of information would result in disclosure of a particular category of information or would be harmful to a public or private interest. These exceptions are set out in **sections 14 to 27** of the Act.

This chapter explains the various exceptions which require or allow a public body to refuse to disclose information to an applicant who makes a request under the Act.

It is important to remember that a basic principle of the FOIPP Act is to give the public access to the records of a public body. Any exceptions to the right of access should be applied in a limited and specific way to provide as much access to information as possible.

Generally, an applicant has a right of access to all or part of any record that is the subject of the request. Refusal to disclose all or part of a record will occur only where the Act provides a specific exception to releasing all or part of a record.

A record cannot be withheld simply because its title or nature indicates that it may contain sensitive information. As well, access cannot be denied because disclosure may embarrass a public body or expose it to liability.

Each record must be carefully reviewed, in consultation with program staff knowledgeable about the subject, to determine whether it may be disclosed or whether an exception in the Act applies.

Public bodies should interpret the exception provisions narrowly. Only the specific information that is excepted from disclosure will be withheld. The exceptions in the Act provide the only basis for refusing to disclose information, and public bodies are required to release information unless the Act expressly provides that all or some of the information in a particular record may be excepted from disclosure.

More than one exception may apply to all or part of a record. A public body should take into account all relevant factors when considering whether an exception to an applicant's right of access applies to a record. No further exceptions can be applied once the

Commissioner has made a decision on those that have been applied. However, the Commissioner will apply any mandatory exceptions that have not been applied by the public body.

The exceptions may apply to requests for general information and also to requests from an individual for their own personal information.

The majority of requests for review to the Information and Privacy Commissioner under **section 60** of the Act will arise from refusal to provide access. Public bodies should be prepared to document and defend their decisions not to disclose particular information.

Mandatory and Discretionary Exceptions

There are two types of exceptions under the Act – mandatory exceptions and discretionary exceptions.

Mandatory Exceptions

Mandatory exceptions commence with the phrase “the head of a public body shall refuse to disclose.” If information falls within a mandatory exception, a public body must refuse to disclose all or part of the record as required. The only case where a mandatory exception may not apply is where there is a public interest that overrides it as provided in **section 30** of the Act. See Chapter 6 of this publication. The legislation recognizes that certain kinds of information should not be disclosed and provides mandatory exceptions to protect that information.

Mandatory exceptions apply to information if:

- Disclosure would be harmful to the business interests of a third party (**section 14(1)**).
- The information is about a third party and is in a tax record (**section 14(2)**).
- Disclosure would be an unreasonable invasion of personal privacy (**section 15**).
- The information is in a law enforcement record and its disclosure would be an offence under an Act of Canada (**section 18(3)**).
- The information would reveal Cabinet confidences (**section 20**).
- The information is subject to legal privilege and relates to a person other than a public body (**section 25(2)**).
- Disclosure is prohibited by another enactment of Prince Edward Island (**section 5**).

Discretionary Exceptions

Discretionary exceptions to the right of access permit a public body to choose whether or not to withhold all or part of a record. Discretionary exceptions commence with the phrase “the head of a public body may refuse to disclose.” There are eleven discretionary

exceptions:

- Disclosure harmful to individual or public safety (**section 16**)
- Confidential evaluations (**section 17**)
- Disclosure harmful to law enforcement (**section 18(1)** and **(2)**)
- Disclosure harmful to intergovernmental relations (**section 19**)
- Public body confidences (**section 21**)
- Advice from officials (**section 22**)
- Disclosure harmful to the economic or other interests of a public body (**section 23**)
- Testing and audit procedures (**section 24**)
- Legal and other privileged information of a public body (**section 25**)
- Disclosure harmful to the conservation of heritage sites, etc. (**section 26**)
- Information that is or will be available to the public (**section 27**)

Discretionary exceptions require two decisions by a public body:

- A factual determination must be made as to whether information falls within the category of information that may be withheld from disclosure.
- The head of the public body must exercise their discretion as to whether information should be withheld.

Harm

Some discretionary exceptions are based on a harms test. This generally provides that access to all or part of a record may be refused if disclosure could reasonably be expected to harm a particular public or private interest.

Harm is defined as “damage” or “detriment” and each exception is designed to prevent the occurrence of particular “harms.” These are discussed in detail in the individual sections of this chapter dealing with the exceptions.

A number of considerations are involved in making a judgment as to harm, but three general factors should be taken into account by public bodies in making such decisions. These are the degree to which the harm is specific, current and probable.

Specific

Is it possible to identify the detrimental effect on the interest or actual party that will suffer harm? To qualify, the injury cannot be a vague general harm.

Current

Is it possible to identify the detrimental effect at the time the exception is claimed or in the foreseeable future? Records which have been protected from disclosure in the past should

be reassessed when a new request is received to ensure that the previously identified harm is still a factor.

Probable

Is there a reasonable likelihood of the harm occurring?

Other Discretionary Exceptions

In a few discretionary exceptions, the basis of the exception is that disclosure would reveal a certain class of information, such as advice from officials or the substance of *in camera* meetings. In such cases there is no need to address the harm that the disclosure may cause, although this may be a factor in exercising discretion.

Exercise of Discretion

The exercise of discretion is fundamental to applying the Act. The Act is based on the principle that the public has a right of access to information in the custody or under the control of public bodies. Subject to limited and specific exceptions, information should not be withheld unless there is an overriding harm or another sound reason for non-disclosure identified in one of the Act's exceptions.

A discretionary exception requires a public body to determine whether harm is likely to result from the release of information that falls within the exception or, if the exception does not have a harms test, whether the interest outlined in the exception should be protected. If no harm is apparent or the particular interest is not adversely affected, the principle and spirit of the Act dictate that the public body should release the information.

The exercise of discretion requires the head, or staff member delegated to make such decisions, to weigh all factors, and consult with other public bodies if appropriate, in determining whether or not information that qualifies for a discretionary exception should be withheld. The exercise of discretion is not a mere formality where there is a cursory examination before the appropriate authority denies access. The public body must be able to show that the records were reviewed, that all the relevant factors were considered and, if the decision is to withhold the information, that there are sound reasons to support the decision.

If there is a request for review, the Information and Privacy Commissioner decides whether or not an exception applies in a particular circumstance. If a discretionary exception has been properly applied, the Commissioner cannot overrule the head's decision. The Commissioner can, however, require the head to reconsider a decision if it appears that the obligation to exercise discretion has been disregarded, or where discretion has been exercised without due care and diligence or for an improper or irrelevant purpose.

Once a public body has determined that all or part of a requested record falls within a discretionary exception, the public body must decide whether to release the information

despite the existence of grounds for refusal. In making a decision, the public body must take into account all the relevant circumstances, as well as advice solicited from within the body, from other public bodies and from other affected parties.

A public body exercises discretion to withhold information on a request-by-request basis, with specific reference to the information requested and the particular circumstances of the case.

A public body must not replace the exercise of discretion with a blanket policy that information will not be released. However, public bodies can develop guidelines to help guide the exercise of discretion, provided they are not interpreted as binding rules.

Some factors that should be taken into account when exercising discretion include:

- The general purposes of the Act; public bodies should make information available to the public, and individuals should have access to personal information about themselves.
- The wording of the discretionary exception and the interests which the exception attempts to balance.
- Whether the applicant's request may be satisfied by severing the record and providing the applicant with as such information as is reasonably practicable.
- The historical practice of the public body with respect to the release of similar types of records.
- The nature of the record and the extent to which the record is significant or sensitive to the public body.
- Whether the disclosure of the information will increase public confidence in the operation of the public body.
- The age of the record.
- Whether there is a definite and compelling need to release the record.
- Whether Commissioner's orders have ruled that similar types of records or information should or should not be disclosed.

Whether an exception is mandatory or discretionary in nature, the public body must consider whether **section 30** of the Act, disclosure in the public interest, requires release of the information. (See Chapter 6 of this publication.)

Application of Exceptions

There is a general process that should be followed in applying all exceptions. There are five basic steps.

Step 1: Preliminary Examination

Undertake a general review of the record(s) to determine which exceptions may apply and

to gauge the complexity of the case and the notices that will be required as part of the process.

Step 2: Detailed Review

Review the record(s) line by line to consider more thoroughly the nature and extent of the exceptions involved. Identify information subject to mandatory exceptions, where a public body has no discretion to disclose information, and information to which no exception applies.

Step 3: Exercise of Discretion

Where discretion is permitted, undertake any necessary consultation and decide, with respect to information where exceptions apply, whether any or all of the information will be refused.

Step 4: Severing

Sever that part of the record(s) to which the public body has decided that it is necessary to refuse access. This will leave a record with a number of blank spaces annotated with references to the section(s) of the Act applied to sever the record, or, if a sequence of pages has been severed, with a single page listing the exceptions applied.

Step 5: Response to Applicant

Prepare a response to the applicant following the guidelines provided in Chapter 3 of this publication. Many exceptions are complicated. Reference should be made to the detailed advice provided in this chapter on the application of each of the specific exceptions.

4.2 RELATIONSHIP TO OTHER ACTS

Paramountcy

Section 5(2) states that if a provision of the FOIPP Act conflicts with another enactment, the FOIPP Act prevails unless:

- Another Act; or
- A Regulation under the FOIPP Act expressly states that the other Act or regulation, of a provision of it, prevails.

It will be necessary to compare the legislative provisions of a particular Act with the exception provisions of the FOIPP Act. If they are comparable and of the same intent so that no conflict arises between them as to what will be disclosed and refused, then the

appropriate section of the FOIPP Act may be cited as a basis for refusing to disclose a record or part of a record.

However, if conflict does arise, it is necessary to determine whether or not the other Act has provisions or regulations made under it that permit its criteria for refusal of access to prevail over the FOIPP Act.

If this is the case, the public body must refuse disclosure under the provision of the other legislation. If this is not the case, then the decision concerning access *must* be based solely on the provisions of the FOIPP Act.

Copyright Act

Section 32.1 of the *Copyright Act* (Canada) states that disclosure of a record pursuant to the *Access to Information Act* (Canada), or disclosure pursuant to any like Act of the legislature of a province, does not constitute an infringement of copyright. Public bodies are not infringing copyright by disclosing copyright material in response to a FOIPP request.

4.3 DISCLOSURE HARMFUL TO BUSINESS INTERESTS OF A THIRD PARTY

The third party bears the burden of proof meaning it is the third party that must provide sufficient evidence that all three parts of section 14(1) are present.

Section 14(1) creates a mandatory exception for information which, if disclosed, would reveal certain types of third party information supplied in confidence, and could also result in one or more specified harms.

The Act provides that the head of a public body must refuse to disclose to an applicant information:

- That would reveal:
 - Trade secrets of a third party; or
 - Commercial, financial, labour relations, scientific or technical information of a third party

That is supplied, explicitly or implicitly, in confidence, if its disclosure could:

- Reasonably be expected to harm significantly the competitive position or interfere significantly with the negotiating position of the third party;
- Result in similar information no longer being supplied to the public body

when it is in the public interest that similar information continue to be supplied;

- Result in undue financial loss or gain to any person or organization; or
- Reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

Section 14(1)(a)(b) and (c) provides a three-part test. The information in question must:

- Be of a type set out in 14(1)(a)
- Be supplied by the third party in confidence 14(1)(b)
- Meet one of the harms or other conditions set out in 14(1)(c)

Type of Record (section 14(1)(a))

In interpreting **section 14(1)(a)** the following concepts apply:

Third party business information is *explicitly* revealed if the information disclosed is itself third party business information or if it makes direct reference to third party business information. Third party business information is *implicitly* revealed if the information disclosed allows a reader to draw an accurate inference about third party business information.

Trade secret is defined in **section 1(n)** of the Act as information, including a formula, pattern, compilation, program, device, product, method, technique or process:

- That is used, or may be used, in business or for any commercial purpose.
- That derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use.
- That is the subject of reasonable efforts to prevent it from becoming generally known.
- The disclosure of which would result in significant harm or undue financial loss or gain.

Information must meet all of these criteria to be considered a trade secret.

Information that is generally available through public sources (e.g., corporate annual reports) would not usually qualify as a trade secret under the Act. A third party must also own trade secrets or must be able to prove a claim of legal right in the information (e.g., a licence agreement) in order for that information to qualify for the exception.

A *third party* is defined in **section 1(m)** of the Act as any person, group of persons or organization other than the applicant (ex., the person making an access request) or a public body.

The other terms in this section have their normal dictionary meanings. *Commercial information* covers information concerning the sale, purchase or exchange of goods or services, such as pricing structures, market research, business plans, and customer records.

Financial information relates to money and its use or distribution or to assets with monetary value such as securities or stock options. Common examples are financial forecasts, investment strategies, budgets, and profit and loss statements.

Labour relations information relates to the management of personnel by a person or organization other than the applicant, whether or not the personnel are organized into bargaining units. Common examples of labour relations information are hourly wage rates, personnel contracts and information on negotiations regarding collective agreements.

Scientific information relates to experiments, principles and procedures derived by scientific method, including information such as designs for a product and testing procedures for drugs.

Technical information relates to particular subjects, crafts or professions that are based on a specific technique or approach. Examples are system design specifications and the plans for an engineering project.

Supplied “In Confidence” (section 14(1)(b))

Section 14(1)(b) covers information provided voluntarily by a third party and information provided by a third party under law or some other form of compulsion.

The information would normally have to be supplied by the third party and not compiled by the public body or generated jointly through negotiation with the public body. However, there may be exceptions where the information supplied to the public body during negotiations remains relatively unchanged in an agreement or could be inferred from an agreement.

For example, a report created by an inspector visiting a plant would not qualify as being supplied by the third party. On the other hand, a letter created by a public body might contain information that would qualify for exception if it reproduces or analyzes information supplied by a third party in such a way as to reveal the information itself. Commercial information in a partnership agreement might also qualify for the exception if the information was originally supplied by a party to the agreement and has remained relatively unchanged in the agreement.

Implicitly in this context means that both parties understand the confidentiality. There may be no actual statement of confidentiality, no written agreement or other physical evidence

of the understanding that the information will be kept confidential. In such cases, all relevant facts and circumstances need to be examined to determine whether or not there is an understanding of confidentiality.

Explicitly in this context means that there is documentary evidence that indicates that information was supplied on the understanding that it would be kept confidential.

In confidence usually describes a situation of mutual trust in which private matters are related or reported.

Some factors that may be considered when determining whether information was supplied implicitly or explicitly in confidence are:

- Whether or not an explicit indication of confidentiality exists.
- The representations of the third party in reply to a third party notice as to their understanding of confidentiality.
- Past practice of the public body, particularly whether similar information has normally been kept confidential in the past.
- The type of information, including the confidentiality with which it is maintained by the third party.
- Whether the information was supplied voluntarily by the third party, at the request of the public body, or as required by law, and the consequences for the third party if it does not supply the information.
- Actions taken by, or conduct of, the public body and third party, which may indicate an understanding of confidentiality.

This guidance is provided to help a public body determine whether information is supplied in confidence. Where this is normal practice, persons and organizations submitting such information should be asked to mark records or parts of records as being submitted “in confidence.”

It is the public body’s responsibility to prove that information was submitted in confidence. It is not sufficient simply to accept a third party’s stamp that documents are confidential or the assertion in representations that information was supplied in confidence. There must be evidence, such as that referenced above, to support the assertion or marking and to prove that the information has been treated consistently in a confidential manner.

Public bodies should review their understandings with third parties concerning the provision of information in confidence.

Effect on Business Interests (section 14(1)(c))

In applying **section 14(1)(c)**, there must be objective grounds for believing that one of the

results listed below will occur as a consequence of disclosure. It must be shown that disclosure of the information would:

- Significantly harm the third party's competitive position;
- Interfere significantly with the third party's negotiating position;
- Result in information no longer being supplied;
- Result in undue financial loss or gain to any person or organization; or
- Reveal information concerning the resolution of a labour relations dispute.

A refusal of access under this exception should be supported by detailed evidence showing that the expectation of harm is reasonable and the harm is probable. The evidence must show that:

- There is a clear cause and effect relationship between the disclosure and the alleged harm.
- The expected harm amounts to damage or detriment and not simply hindrance or minimal interference.
- The likelihood of harm from disclosure of the specific information is genuine and conceivable, and not merely speculative; it is not sufficient to show that there is a potential for harm simply because the information is sensitive.

Harm Significantly the Competitive Position of a Third Party (section 14(1)(c)(i))

Harm *significantly* means that disclosure of the information will damage or cause detriment to the third party's competitive position and that the damage or detriment will have considerable impact on the third party involved.

In order to assess the significance of the harm, a public body should review, among other things:

- the nature of the information itself;
- the third party's representations regarding the harm involved;
- an objective appraisal of that harm, including any monetary or other value placed on it, if this can be determined;
- the impact on the third party and its ability to withstand this;
- and any public interest, as set out in **section 30**, which may affect the decision concerning disclosure.

Interfere Significantly with the Negotiating Position of a Third Party (section 14(1)(c)(i))

This provision allows for situations where disclosure of third party information would have

a major impact on ongoing or future negotiations. Completed negotiations are not normally subject to the exception unless there is a good probability that the particular strategies will be used in the future and the disclosure of information relating to completed negotiations would reveal such strategies.

The intent of the provision is to protect a third party's ability to negotiate effectively with either the public body or other parties.

Examples would include negotiating positions, options, instructions and pricing criteria, and points used in negotiations.

Result in similar information no longer being supplied to the public body when there is a continuing public interest that similar information continued to be supplied (section 14(1)(c)(ii))

This provision allows for situations where a third party may be so concerned by the possibility that information may be released that it refuses to supply similar information in the future. There must be a continuing public interest in the particular information being supplied. If this is the case, a public body can consider whether disclosure would discourage either the particular third party or another third party from voluntarily supplying information to it or other public bodies.

A third party may assert that it will no longer provide information if it may be released under the FOIPP Act. However, the public body is required to come to a reasonable decision as to whether or not this will be the case. It is unlikely that similar information will no longer be supplied where the third party has a financial or other incentive to continue supplying the information or where it is legally required. Examples include voluntary supply of pricing information by a group of third parties which serves to effectively regulate pricing of products, and provision of information on leases and rental values of commercial property in order to apply market-value assessment across a city.

Undue Financial Loss or Gain to any Person or Organization (section 14(1)(c)(iii))

For this provision to apply, there must be objective grounds for believing that releasing the information would result in an undue loss or gain measured in monetary or monetary-equivalent terms (ex., loss of revenue, loss of corporate reputation or loss of good will).

The undue financial loss or gain may apply to the public body that has custody or control of the information in question, the third party that supplied the information or any other person or organization.

There must be objective grounds for believing that the harm contemplated by this exception would actually result from disclosure. In refusing access under this provision, a public body should be prepared to present detailed and convincing evidence of the facts that led to the expectation that harm would occur if the information were disclosed. A link is required

between the disclosure of specific information and the harm that is expected from the release.

Reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute (section 14(1)(c)(iv))

This provision protects information which itself explicitly reveals a report of an arbitrator or other such person or directly makes reference to such a report, or which implicitly reveals information about such a report, by allowing a reader to draw an accurate inference about it. The report would have to deal with a labour relations dispute of a third party, not a public body.

A *report* may include a broad range of records providing information or opinions, or consisting of a formal statement or account of the results of an analysis of information. The recording of mere observation or a simple statement of fact would not generally be covered by this provision. The provision requires that an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute create the report. An *arbitrator* is generally considered to be a neutral person chosen by the parties to a dispute to hear their arguments and give judgment between them. The parties may submit themselves voluntarily or under a compulsory agreement to the decision of this person. A *mediator* is a person who facilitates discussion between parties who disagree with the aim of reconciling them. A *labour relations officer* is any person appointed to inquire into or resolve any form of labour relations dispute or issue.

Other persons or bodies appointed to resolve or inquire into a labour relations dispute includes any person or body appointed by any level of government or any public body; for example, Cabinet appointments, ministerial appointments, appointments by the council, board or the chief executive officer of a public body.

Tax Information

Section 14(2) provides that a public body must refuse to disclose information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax. This is a mandatory exception and the public body has no discretion to release the information unless required to do so by law or by the provision in **section 30** for disclosure in the public interest.

Information collected on a tax return is information on a form used to determine taxes to be paid for municipal, education, provincial or federal purposes, and includes corporate, business and personal tax information of a third party (see also section 4.4 of this chapter).

Collected for the purpose of determining tax liability means collected for the purpose of determining whether a person or organization owes past, present or future taxes to a municipal, provincial or federal government.

Collected for the purpose of collecting a tax means collected by authorities for the purpose of collecting due or overdue taxes for the municipal, provincial or federal government.

Section 14(2) may not be used to withhold an applicant's own tax information, since this is information about the company, organization or individual (e.g., sole proprietor) and not information about a third party.

This type of information commonly includes tax data derived from tax forms, audits of a business intended to determine whether or not taxes are owed, and information about directors of a bankrupt corporation gathered to determine who should be liable for taxes that are in arrears.

The exception may be used in relation to information concerning royalties or obtained in the process of collecting royalties. However, such royalties must have a statutory basis as a tax. Where there is doubt about the nature of a royalty, legal advice should be sought.

When the Exception Does Not Apply

Section 14(3) provides for situations where the exceptions set out in **section 14(1)** and **(2)** do not apply:

If the Third Party Consents to Disclosure

A public body cannot withhold requested information under this exception when the third party concerned has consented to disclosure, although other exceptions may be applied to the information. Consent should be in writing. For details on consent see Chapter 5 of this publication dealing with third party notices.

If the third party neither consents nor objects to disclosure, the public body must assess the appropriate application of this exception. It always remains the responsibility of the public body to make the final decision, taking into consideration all relevant circumstances.

If an Enactment of Prince Edward Island or Canada Authorizes or Requires Disclosure of the Information

The information must be released where disclosure is provided for in other federal or provincial legislation.

If the Information Relates to a Non-Arm's Length Transaction between the Government of Prince Edward Island and another Party

This provision applies in circumstances where the Government of Prince Edward Island is a direct participant in a transaction and is working with the other party.

The definition of a non-arm's length transaction in **section 4(3)** of the Act is not applicable to this section. In this case, a *non-arm's length transaction* is a transaction between unrelated parties that has characteristics comparable to a transaction between related persons. The parties may be influenced in their bargaining by something other than individual self-interest, or one of the parties may have sufficient leverage or influence to exercise control or pressure on the free will of the other.

An example would be an agreement between a corporation and the Government of Prince Edward Island to invest in and pursue a project together. In this section, the *Government of Prince Edward Island* includes departments, branches and offices of the government and any agencies, boards, commissions, corporations, offices or other bodies designated as public bodies in **Schedule 1** of the FOIPP Regulations.

If the Information is in a Record that is in the Custody or under the Control of the Public Archives and Records Office and has been in Existence for 50 Years or more

This provision recognizes that the sensitivity of business information decreases with time, and so does the injury that might occur to the business interests of a third party as a result of disclosure.

The fact that such information resides in the Public Archives and Records Office means that it is information important for research and historical purposes and that it should be available for those purposes after the passage of 50 years.

Disclosure of information can take place earlier if it would not be harmful to the business interests of a third party. See Chapter 7.11 of this publication for disclosure of information in archives.

4.4 DISCLOSURE HARMFUL TO PERSONAL PRIVACY

Section 15 of the Act protects the privacy of individuals whose personal information may be the subject of a FOIPP request by someone else. This protection is provided by a mandatory exception for personal information when its release would constitute an unreasonable invasion of an individual's privacy.

In the exception the individual whom the information is about is referred to as a *third party*. This protection applies only to individuals and not to groups, organizations or corporations. The exception must always be considered when an applicant makes a request for someone else's personal information.

Any time someone other than the individual whom the information is about, or their representative, requests personal information as defined in **section 1(i)** of the Act, it must be subjected to a test to determine whether disclosure would be an unreasonable invasion

of a third party's personal privacy.

Definition of Personal Information

Personnel information is defined as recorded information about an identifiable individual. A detailed definition is provided in Chapter 1.5 of this publication. It is important to remember that the definition is non-exhaustive. The examples given are purely illustrative and do not define personal information in its entirety.

To qualify as personal information under the Act, information must be written, photographed, recorded, or stored in some manner. Information conveyed in a conversation that is not recorded does not constitute personal information for the purposes of the Act. The personal information must be about an *identifiable individual*. It must be about an individual and not about a group of individuals, an organization or a corporation. The individual may be named in the record or it may be possible to ascertain or deduce the identity of the individual from the contents of the record.

Exception for Personal Information

Section 15(1) establishes a mandatory exception for personal information if disclosure of it would be an unreasonable invasion of a third party's personal privacy. When this is the case, the public body has no discretion to release the information.

Disclosure Not an Unreasonable Invasion of a Third Party's Privacy

Section 15(2) sets out those circumstances when disclosure of personal information is considered not to be an unreasonable invasion of a third party's personal privacy. In these circumstances, a public body may not rely on **section 15** to refuse disclosure of personal information. However, other sections of the Act should still be considered when making a decision about disclosure.

Section 15(2) states that disclosure of personal information is not an unreasonable invasion of an individual's personal privacy if:

- The third party has, in writing, consented to or requested the disclosure;
- There are compelling circumstances affecting anyone's health or safety, and written notice of the disclosure is given to the third party;
- An Act of Prince Edward Island or Canada authorizes or requires the disclosure;
- The disclosure is for research or statistical purposes and is in accordance with **sections 39 and 40** (research is discussed in Chapter 7 of this publication);
- The information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body;
- The disclosure reveals financial and other details of a contract to supply goods or

- services to a public body;
- The disclosure reveals details of a licence, permit or other similar discretionary benefit that has been granted to a third party by a public body and relates to either a commercial or professional activity or to real property;
- The disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body; or
- The personal information is about an individual who has been dead for 25 years or more.

The provisions of **section 15(2)** are discussed in more detail below.

Consent (section 15(2)(a))

Personal information may be released where the individual either consents to or requests the disclosure. This consent or request must be in writing and must be specific. Consent in such circumstances normally comes after third party consultation. Implied consent is not sufficient to satisfy this condition. Consent can be provided to the public body on behalf of the individual by certain persons and under certain conditions as set out in **section 71** of the Act. The exercise of rights by others is discussed in detail in Chapter 7 of this publication.

Health and Safety (section 15(2)(b))

This provision applies only when there are compelling circumstances affecting the health or safety of someone other than the third party. A *compelling circumstance* is one where there is no other way to protect someone else's health and safety, or where there is an emergency and disclosure is the fastest, most direct way to protect someone else's health or safety. The release of the information requested must also be likely to have a direct bearing on a compelling health or safety matter and it will be necessary to show this.

In applying this provision, the public body is required to mail a notice of disclosure to the last known address of the third party whose personal information the public body is disclosing. This is the last address on file with the public body, unless circumstances are such that another public body or level of government may have a more recent address. The public body is required to make reasonable attempts to determine the address of the third party.

Privacy laws should not handcuff emergency management. If a provincial employee is well-intentioned, but does not understand what a public body may do in an emergency situation, it may result in distress and delays. See also section 15(2) (c), 15(5)(b), 30, 37(1)(q), (cc) of the FOIPP Act, and section 5 and schedule 3 of its regulations.

Act of Prince Edward Island or Canada (section 15(2)(c))

This provision states that personal information may be disclosed if disclosure is authorized or required by provincial or federal statute.

Research Purposes (section 15(2)(d))

This provision permits the disclosure of personal information for research or statistical purposes in accordance with provisions set out in **sections 39 and 40** of the Act. This recognizes that research may legitimately require the use of identifiable personal information, but ensures that the privacy rights of research subjects are protected. Researchers have to comply with a stringent set of conditions. A full discussion of research agreements appears in Chapter 7.10 of this publication.

Employment Information About Public Officials (section 15(2)(e))

This provision sets special conditions for the release of particular employment information about officers, employees or members of public bodies. The rationale is that more information should be available about individuals who are paid out of public funds.

Section 1(c) defines employee as including a person who performs a service for the public body as an appointee, volunteer or student or under a contract with the public body.

The provision establishes that the disclosure of information about the actual job classification and responsibilities of an employee, and information about the duties or job description for the position occupied is not an unreasonable invasion of an individual's personal privacy. This also applies to the release of the salary range for the position.

Where no salary range exists, public bodies should consider creating one in order to support release of information that promotes more accountability for the expenditure of public funds. The provision also establishes that the disclosure of a discretionary benefit provided on an individual basis, rather than in accordance with a plan, scale or formula, including any allowance with monetary value that the public body chooses to provide, is not an unreasonable invasion of an individual's privacy.

Contracts for Goods and Services (section 15(2)(f))

This provision establishes that the release of financial and other details about the supply of goods and services to a public body is not an unreasonable invasion of privacy, even when such details may be personal information. The rationale is that the public is entitled to know from whom and for what amount such services were purchased. This is an important part of public accountability.

Financial details relate to the amounts paid under the contract.

Other details include the names of the parties, the subject of the contract and its terms and conditions.

Contract to supply goods and services refer to an agreement concluded by a public body with a third party to buy or sell products, merchandise, or services, as well as to an agreement entered into by a public body in relation to employment or performance of work-related duties. It does not apply where a public body provides money to a third party to provide contracted services to a party other than a public body.

In releasing this type of information, public bodies should ensure that they are not disclosing information that may qualify for protection under **section 14**, information the disclosure of which would be harmful to third party business interests.

Licence, Permit or Similar Discretionary Benefits (section 15(2)(g))

This provision establishes a mechanism for releasing information about discretionary benefits granted by a public body to a third party. Again the rationale is to ensure accountability on the part of public bodies with respect to monetary and other benefits that fall within its discretion. Disclosure is limited to licences, permits or discretionary benefits relating to a commercial activity or to real property.

Licence or permit means authorization to carry out an activity, such as operating a particular establishment, or carrying on a professional or commercial activity. Examples would include business licences, taxi licences, and building and development permits.

Other similar discretionary benefit refers to both monetary and non-monetary benefits, or allowances given by a public body.

This provision does not allow disclosure of a licence or permit of a personal nature, such as a recreational fishing or hunting licence, a dog licence or a camping permit. The benefit must be discretionary, that is, the public body must have a choice as to whether or not to provide the benefit or allowance. The power to suspend, cancel or reinstate a licence or permit is an indication that the licence or permit is a discretionary benefit. So too is the power to limit or allocate permits by setting formulae or limiting numbers.

Disclosure under this provision must reveal only the name of the person to whom the licence, permit or discretionary benefit is provided, and the nature of the benefit. It must not include personal information supplied in support of the application for the benefit.

Discretionary Benefit of a Financial Nature (section 15(2)(h))

This provision enables disclosure of information about a discretionary financial benefit provided to an individual by a public body.

A discretionary benefit of a financial nature is any monetary allowance that the public body chooses to provide (ex. a scholarship or a grant). Information regarding eligibility for income assistance or social benefits, or regarding the determination of individual benefit levels, is not covered by this provision since these benefits are calculated according to entitlement formulae.

Background personal information required by the public body or provided voluntarily by the applicant must not be released under this provision. An example of this type of disclosure would be the disclosure of records that show that an individual has received a grant from a public body, the amount of the grant and the purpose for which the grant will be used. Personal information supporting the application for the grant itself would not be disclosed.

Individual Dead for 25 Years or More (section 15(2)(I))

This provision puts a time limit on the protection of privacy after death. Once an individual has been dead 25 years or more, release of their personal information is deemed not to be an unreasonable invasion of the individual's privacy. The provision is particularly important for permitting historical and genealogical research.

The onus is on the applicant to produce evidence that an individual has been dead for 25 years or more.

Section 15(2)(j) is subject to subsection (3), the disclosure is not contrary to the public interest and reveals only the following information about a third party:

1. Enrolment in an English or French School system (defined in the *School Act*)
2. Admission to a health care facility or institution unless it would reveal the treatment
3. Attendance or participation in a public event/activity as described
4. Receiving an honour or award

When considering a request to which **section 15(2)(j)** may apply, public bodies must take into account the circumstances surrounding the request. If the requested information could be used to commit a criminal act or harm an individual or property, then it is likely to be contrary to the public interest to disclose the information. If a disclosure would reveal information about the mental or physical health of individuals, or affect their mental or physical health, the disclosure may be contrary to the public interest.

Enrolment in a School or an Educational Body, or in a Program of a Post-Secondary Educational Body (section 15 (2)(j)(i)).

This provision allows a school board, charter school or regional authority (all as defined in the *School Act*) to confirm that an individual is or was enrolled in a school under its jurisdiction. A post-secondary educational body can confirm that an individual is or was enrolled in a specific program at that institution. Educational bodies may also provide lists or class photographs of the individuals enrolled in a particular school or post-secondary program whether currently or in the past (ex. the students in a particular high school or the students in a particular apprenticeship program). This facilitates school or program reunions. This provision does not allow disclosure of whether a school or post-secondary institution at a particular individuals' timetable of studies or other personal program. Attendance at or participation in a public event or public activity **Section 15(2)(j)(iii).**

This provision allows disclosure of the names of individuals who are recorded as having attended or participated in a public event or activity. A public event or activity is something that is noteworthy, supervised or organized in some way. It would be open, or accessible, to the public

- Without restriction,
- With limited attendance due to space or safety concerns, or
- Through ticket sales.

The fact that someone was simply observed or something was seen happening does not make an occasion a public event or activity. The Act is based on recorded information, so a record of the attendance or participation is needed for disclosure under this provision. **Section 15(2)(j)(iii)** does not relate to:

- Events or activities that are organized or sponsored by a third party that may be renting a facility owned by a public body.
- Events that are not authorized or sponsored by a public body; or
- Activities of arm's-length bodies such as "Foundations" or "Friends" unless the record is in the custody of the public body

Disclosure is not limited to current events, information relating to past events may be disclosed if records exist. Photographs taken at the event may be disclosed under **section 15(2)(j)(iii)**. It is important that reasonable steps are taken to ensure the accuracy of records of such activities that are maintained by public bodies.

Receipt of an honour or award granted by or through a public body **Section 15(2)(j)(iv)**. This provision allows the disclosure only of information concerning the receipt of an honour or award. This means that the individual must have actually received the honour or award. **Section 15(2)(j)(iv)** does not allow disclosure of an offer of, or qualification for, an honour or award if the honour or award was not presented, or if the honour or award was declined. The provision also does not allow disclosure of contact information about the recipient (ex.. home address) unless the recipient has consented in writing to this disclosure.

A public body can confirm that a particular honour or award has been given to an individual and can disclose a list of names of individuals who have received a particular honour or award. Disclosure of a photograph of an individual named as a recipient of a current or past award would also be allowed under this provision.

Existence of Record

In some instances, disclosure of the mere fact that a public body maintains a record on a third party may be an unreasonable invasion of a third party's privacy.

Section 10(2)(b) of the Act provides that a public body may, in response to an applicant, refuse to confirm or deny the existence of a record containing personal information about a third party, if disclosing the existence of the information would be an unreasonable invasion of the third party's personal privacy.

Most public bodies will use this provision in rare instances. However, public bodies that hold sensitive personal information, such as medical or financial information, may routinely refuse to confirm or deny the existence of records containing personal information about a third party.

When the existence of a record is neither confirmed nor denied, the response to the applicant required under **section 10(1)** must indicate that the public body is unable to confirm or deny the existence of the requested records and that, if such records did exist, they would be excepted from disclosure under **section 15** of the Act (disclosure harmful to personal privacy). The response must also provide the contact information of someone who can answer questions about the decision and that the applicant can ask the Commissioner for a review.

A refusal to confirm or deny the existence of a record is a significant limit to the right of access. If an applicant asks the Information and Privacy Commissioner to review a refusal to confirm or deny the existence of a record, the public body will be required to provide

detailed and convincing reasons why **section 10(2)** was applied.

Before refusing to confirm or deny the existence of a record, a public body is expected to determine whether or not any record exists in order to properly fulfil its duty to assist the applicant.

Application of Exception

A detailed explanation of the procedures relating to third party notice which apply to this exception is provided in Chapter 5 of this publication.

Section 15(3) states that under clause 2(j) disclosures would be unreasonable if the third party has requested the information not be disclosed.

Disclosure an Unreasonable Invasion of a Third Party's Privacy (Section 15(4))

There are particular types of personal information the disclosure of which is presumed to be an unreasonable invasion of a third party's personal privacy. That is to say, the legislation indicates that there is a likelihood that disclosure of such information might lead to an unreasonable invasion of privacy.

This provision creates a presumption that may be overridden by evidence to the contrary. In such instances, the burden of proof is on the applicant to provide evidence that could override the presumption.

Section 15(4) provides that disclosure of personal information is presumed to be an unreasonable invasion of a third party's privacy if the personal information:

- Relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation.
- Was compiled and is identifiable as part of a law enforcement matter, except to the extent that disclosure is necessary to prosecute in respect of, or to continue or conclude the matter.
- Relates to eligibility for income assistance or social services benefits or to the determination of benefit levels.
- Relates to an individual's employment or educational history.
- Was collected on a tax return or gathered for the purpose of collecting a tax.
- Consists of an individual's bank account information or credit card information.
- Consists of personal recommendations or evaluations.

- Character references or personnel evaluations.
- Consists of the third party's name when:
 - It appears with other personal information about the third party; or
 - The disclosure of the name itself would reveal personal information about the third party; or
- Indicates the third party's racial or ethnic origin, or religious or political beliefs or associations.

Generally, these types of personal information tend to be of a particularly sensitive or delicate nature. In interpreting this provision, the following explanations should be considered.

Medical, Psychiatric or Psychological Information (section 15(4)(a)) covers records relating to an individual's physical, mental or emotional health, including, for example, diagnostic, treatment and counselling information.

Law Enforcement (section 15(4)(b)) covers investigations and proceedings relating to offences under the *Criminal Code* (Canada), breaches of other federal and provincial statutes and regulations, contravention of municipal by-laws, and formal security or administrative investigations carried out by a public body.

Disclosure of personal information in a law enforcement record is not presumed to be an unreasonable invasion of privacy if disclosure is necessary to prosecute in respect of the law enforcement matter or to continue or conclude the investigation.

This provision recognizes that a public body that is in possession of evidence relating to a law enforcement matter must have the power to disclose that evidence to the police, another law enforcement agency and to Crown counsel or other persons responsible for prosecuting the offence or imposing a penalty or sanction.

Income Assistance and Social Benefits (section 15(4)(c)) relates to monetary benefits provided by governments to augment an individual's earnings, as well as non-monetary contributions that help supplement earnings from another source. Disclosure of such information is presumed to be an unreasonable invasion of personal privacy.

Relate here means that a connection or association must be established between the personal information and the eligibility or determination.

Eligibility means that the personal information must relate to whether a person qualifies to receive income assistance or social service benefits.

Determination of benefit levels means that the personal information must relate to a

determination of how much benefit a person receives.

Employment History (section 15(4)(d)) refers to any information regarding an individual's work record, including the name of an employer, past and present, the term of employment, the duties associated with a position, the salary and reasons for leaving, and any evaluation of job performance. This presumption of unreasonable invasion of privacy does not apply to some employment information about officers, employees and members of public bodies (see Employment information about public officials (**section 15(2)(e)**)).

Educational History (section 15(4)(d)) refers to any information regarding an individual's schooling and formal training, including names of schools, colleges or universities attended, courses taken, and results achieved.

Personal Information Collected on a Tax Return or Gathered for the Purpose of Collecting a Tax (section 15(4)(e)) means personal information on a form used to calculate or report tax to be paid. It applies whether the tax return form was used to collect municipal, federal, or provincial taxes.

Gathered for the purpose of collecting a tax means collected by authorities for the purpose of collecting due or overdue municipal, federal, or provincial taxes.

Bank Account and Credit Card Information (section 15(4)(e.1)) refers to an individual's bank account and credit card information. Other information about an individual's financial history, such as assets, liabilities and credit history, falls within the definition of personal information and is also subject to the unreasonable invasion of privacy test. **Section 15(4)(e.1)** is intended to address concerns about the handling of electronic credit transactions and the possible misuse of credit card numbers.

Personal Recommendations, Evaluations, and Character References (section 15(4)(f)) refers to both the assessment of employment potential and vouching for an individual's good character within the employment context. A formal process of conducting the assessment or evaluation is implied. Personnel evaluations arise most often in the employment context and include job performance appraisals and absenteeism reports.

Name of Individual (section 15(4)(g)) refers to situations where disclosure of an individual's name can be an unreasonable invasion of personal privacy if it is connected to other information about the individual. The name by itself may have attributes that reveal information about the individual (ex. gender, race or ethnic origin).

Racial or Ethnic Origin or Religious or Political Beliefs or Associations (section 15(4)(h))

Racial origin means information identifying common descent that connects a group of persons (ex. Mongolian race or Caucasian descent).

Ethnic origin is similar to racial origin in that it identifies a common descent that connects a group of persons but extends to other common attributes such as language, culture or country of origin.

Religious or political beliefs refers to an individual's opinions about religion or a political party, an individual's membership or participation in a church, a religious organization or political party or an individual's association or relationship with a church, a religious organization or a political party.

Associations refers broadly to relationships with organizations such as labour unions.

Determination of Unreasonable Invasion of Privacy

Section 15(5) of the Act sets out criteria for determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy. It provides that, in determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy under **sections 15(1) and (4)**, a public body must consider all the relevant circumstances.

Although not exhaustive these include:

- The disclosure is desirable for the purpose of subjecting the activities of the Government of Prince Edward Island or a public body to public scrutiny.
- The disclosure is likely to promote public health and safety or the protection of the environment.
- The personal information is relevant to a fair determination of the applicant's rights.
- The disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people.
- The third party will be exposed unfairly to financial or other harm.
- The personal information has been supplied in confidence.
- The personal information is likely to be inaccurate or unreliable.
- The disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant.
- The personal information was originally provided by the applicant.

A list of factors which may be considered under **section 15(5)** were identified by the Alberta Commissioner and have been distributed by the Prince Edward Island Commissioner. These circumstances are not specifically listed in our **section 15(3)** but are factors that may be considered in making a decision under this section. This list was forwarded by the Prince Edward Island Commissioner as follows:

- Disclosure of the information would promote the objective of providing citizens of the Province with an open, transparent and accountable government.
- A third party's refusal to consent to the release of their personal information.
- The fact that an applicant is not required to maintain the confidentiality of personal information once it has been released to them.
- If it is not possible for a public body to notify a third party under **section 38**.
- The fact that personal information is available to the public.
- The fact that the applicant was previously given some other information.
- Whether, under the circumstances, it is practicable to give notice to the third parties if relevant circumstances weigh in favour of not disclosing the personal information of the third parties.
- The fact that the names of individuals requested by the applicant were provided solely in their professional capacity.
- The fact that the names of individuals requested by the applicant were contained in letters sent to the applicant's solicitor.
- If disclosure of the information would affect the applicant's career opportunities it is a relevant circumstance that weighs in favour of disclosing a third party's personal information.
- Where a person who has obtained information in confidence uses that information as a springboard for activities detrimental to the person who made the confidential communications.
- The existence of a power imbalance between the parties.
- The nature and content of the records.
- The fact that the applicant has no pressing need of the third party personal information.

In applying **section 15(5)** a public body should consider not only the specific criteria set out in the provision but all the relevant circumstances. It should consider the sensitivity of the personal information in the context in which it was collected or compiled and the circumstances governing its continued protection or disclosure. For example, the sensitivity of a person's name and address in relation to a contagious disease would normally be protected for a very long period of time. However, if disclosure is necessary to protect public health and safety, the personal information could be disclosed.

Disclosure is permitted if consideration of all the relevant circumstances leads the public body to conclude that the disclosure is not unreasonable in the specific case. As the example demonstrates, the criteria set out in **section 15(5)** may, in exceptional circumstances, dictate the disclosure of the sensitive types of personal information described in **section 15(4)**, despite the fact that disclosure of such information is normally considered an unreasonable invasion of a third party's personal privacy. The provisions of **section 15(5)** are discussed in more detail below.

Public Scrutiny (section 15(5)(a))

This provision recognizes that, in some cases, the desirability of public scrutiny of the internal workings of a public body will prevail over the protection of personal privacy.

Public scrutiny is not necessarily limited to instances where wrongdoing is alleged or where it is alleged that the public body's normal practices and procedures are not being followed. It may be appropriate to disclose some personal information in order to demonstrate that the law is being properly enforced or public policy being carried out.

The public body should consider the broader interest of public accountability that may be advanced by disclosure of the requested information. For example, personal information about a successful job applicant may be disclosed to demonstrate that a qualified individual was appointed to a post and that the competitive process is working in a satisfactory manner.

Public Health, Safety and Protection of the Environment (section 15(5)(b))

These public interests provide powerful override criteria for assuring protection of the general public interest.

Public health refers to the well being of the public at large. The test is whether the level of physical, mental or emotional health of all or a significant part of the public would be maintained or improved by the disclosure of particular personal information.

Public safety refers to the safety or well-being of all or a significant part of the public. This test centers on whether disclosure of personal information would reduce the community's exposure to a particular risk or danger.

Protection of the environment refers to guarding or defending all components of the earth including:

- Air, land, and water

- All layers of the atmosphere
- All organic and inorganic matter
- The interacting natural systems that include components of these things – from degradation through illegal or improper use.

Determination of an Applicant's Rights (section 15(5)(c))

There may be occasions where the applicant requires access to personal information about someone else in order to assist in determining their own rights.

Motives for requesting information are not normally relevant to the processing of a request. However, if it appears that the personal information is being requested for this purpose, it will be necessary for the applicant to confirm that this is the case. The interests of the applicant and the privacy interests of the third party will then have to be weighed to decide whether disclosure of personal information is essential to a fair determination of the applicant's rights.

The disclosure requires that the information be relevant to a fair determination of the applicant's rights. This means that the personal information requested must have a direct bearing on those rights and that, without the personal information, the applicant will probably not be able to resolve outstanding issues in a just and equitable manner. An important factor is whether there are other ways to obtain the required information.

Applicant's rights refers to any claim, entitlement, privilege or immunity of the applicant who is requesting someone else's information. For example, disclosure of third party personal information may be necessary so that an individual can prove their inheritance rights.

If an applicant has agreed to waive future claims on a matter, the applicant has no rights to be determined and cannot rely on this provision to pursue the matter.

Claims, Disputes or Grievances of Aboriginal People (section 15(5)(d))

There may be a need to disclose personal information about individuals in order to research the background and expedite the settlement of wider rights for aboriginal people.

Validating means the confirming of rights that have been contended by the parties to a claim, dispute or grievance.

The phrase *claims, disputes and grievances* is interpreted broadly to include all manner of controversies, debates and differences of opinions regarding issues, and is not restricted to

differences over land claims.

Aboriginal people means individuals whose racial origins are indigenous to Canada.

Exposure to Financial or Other Harm (section 15(5)(e))

There may, from time to time, be circumstances where disclosure of personal information may mean that the individual involved will be exposed unfairly to monetary loss or injury of a similar nature. For example, release of partial or inconclusive test results about an individual may result in loss of their employment. In such circumstances, a public body should opt for protecting personal privacy. Disruption of family relationships or damage to the reputation of deceased individuals may also constitute harm.

Personal Information Supplied in Confidence (section 15(5)(f))

There are circumstances where personal information is supplied in a setting of trust and in the confidence that it will not be disclosed. Sometimes this understanding is more implicit than explicit and, in such circumstances, the public body should attempt to protect the personal privacy of the third party.

Some factors to consider when determining whether or not personal information was supplied in confidence are:

- The existence of a statement or agreement of confidentiality, or lacking this, evidence of an understanding of confidentiality.
- The understanding of a third party as set out in their representations as a result of third party notice.
- Past practices in the public body, particularly in regard to keeping similar personal information confidential.
- The type of personal information, especially its sensitivity and whether it is normally kept confidential by the third party.
- The conditions under which the information was supplied by the third party, voluntarily or through informal request by the public body or under compulsion of law or regulation, and the expectations created by the receipt or collection process.

The burden of determining whether or not information was supplied in confidence lies with the public body. Public bodies should ask their clients and organizations with which they are dealing to mark as confidential any records or parts of records containing personal information which are being supplied in confidence. However, it is not sufficient for a public body to simply accept the stamp or assertion of a third party for confidentiality.

There must be evidence to support the assertion and to prove that the personal information has been treated consistently in a confidential manner.

Inaccurate or Unreliable Personal Information (section 15(5)(g))

A public body may have inaccurate personal information in its custody or under its control for a variety of reasons. It may have been incorrectly recorded at the time of collection or compilation or it may have become inaccurate with the passage of time or as a result of a change in circumstances. For these or other reasons, the public body may be unsure of the reliability of personal information. Such personal information should be disposed of under approved records disposition processes. Otherwise, no personal information should be disclosed from such records until the individual concerned has consented and verified that the information is correct.

Unfairly Damage Reputation (section 15(5)(h))

If disclosure of personal information will unfairly damage the reputation of an individual, it should not be disclosed.

Unfairly has the normal meaning of without justification, legitimacy or equity.

Damage the reputation of a person means to harm, injure or adversely affect what is said or believed about the individual's character. An example would be the disclosure of allegations of sexual harassment against an individual before an internal investigation is concluded.

Personal Information Originally Provided by the Applicant (section 15(5)(i))

The applicant may have provided information about an individual because the individual was in the applicant's care or custody at the time. It is particularly relevant if the applicant and the other individual have no adverse interests at the time of the request. Examples include personal information provided to a public body by an applicant who had guardianship or trusteeship of an individual and provided the information as part of that responsibility.

4.5 DISCLOSURE HARMFUL TO PUBLIC OR INDIVIDUAL SAFETY

Section 16 of the Act allows a public body discretion to refuse to disclose information when the disclosure is likely to threaten individual or public health or safety.

It is a discretionary exception. **Section 16(1)** allows discretion to refuse to disclose information to an applicant if that disclosure could reasonably be expected to:

- Threaten anyone else's safety or physical or mental health; or
- Interfere with public safety.

The exception may extend to an applicant's own personal information as well as to information about third parties.

Threaten means to expose to risk or harm, and *safety* implies relative freedom from danger or risks.

Mental health refers to the functioning of a person's mind in a normal state.

Physical health refers to the well-being of an individual's physical body.

The mental or physical health of a person would be threatened if information were disclosed to an applicant that would cause severe stress to the person's mind or body.

In making determinations about mental or physical health, a public body may consult with its own health or other qualified professional staff, or consult a duly qualified health professional outside the public body to help arrive at a decision.

Individual safety could be threatened if information were released that allowed someone who had threatened to kill or injure the individual to locate them. Examples of individuals whose safety might be threatened would include an individual fleeing from a violent spouse, a victim of harassment or a witness to harassment, an employee who has been threatened during a work dispute or harassment case, and an individual in a witness protection program.

Mental or physical health might be threatened if information were disclosed to the applicant that could cause an individual to become suicidal or that could result in verbal or physical harassment or stalking.

Interference with public safety would occur where the disclosure of information could reasonably be expected to hamper or block the functioning of organizations and structures that ensure the safety and well-being of the public at large.

Section 16(2) specifically allows discretion to refuse to disclose to an applicant their own personal information if the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety. The decision must be supported by the

opinion of a physician, psychologist, psychiatrist or other appropriate expert, depending on the circumstances of the case.

Immediate and grave harm to an applicant's health or safety means serious physical injury or mental trauma or danger to the applicant that could reasonably be expected to ensue directly from disclosure of the personal information. This is an exception that is rarely used. It is important that the exception is based on the immediate and substantial harm that would result from the disclosure of information to the individual.

Section 5 of the FOIPP Regulations governs the use of experts in providing individuals with very sensitive information about themselves. When using this section, the public body must have an agreement in place to ensure that the expert maintains the confidentiality of the information. If a copy of any record is provided to the expert, it must be returned to the public body or disposed of in accordance with the agreement. An example where this exception may be relevant is where an individual with a long and difficult history of mental instability might suffer grave mental or physical trauma if certain diagnoses were made available to them without the benefit of medical or mental health intervention.

Though the intent of **section 16(2)** is to ensure that the applicant does not receive personal information that might cause immediate and grave trauma, efforts should be made to provide to the applicant as much of his or her own personal information as possible. After obtaining the expert opinion, the public body may require that the applicant who has requested access to a record examine that record in person, and in the presence of someone who can clarify the information and assist the applicant in understanding it. That person may be a medical or other expert, a member of the applicant's family, or some other person approved by the public body (**section 5(5)** of the FOIPP Regulations).

Section 16(3) allows discretion to refuse to disclose information that reveals the identity of an individual who has provided confidential information about a threat to someone's safety or mental or physical health. This provision allows a public body to protect the identity of experts and of informants who provide such information.

Existence of Record

In some instances, disclosure of the mere fact that a public body maintains a record may reasonably be expected to threaten someone else's safety, interfere with public safety, or even cause harm to the applicant.

Section 10(2)(a) of the Act provides that a public body can refuse to confirm or deny the existence of a record containing information described in **section 16**.

When the existence of a record is neither confirmed nor denied, the response to the applicant, as required under section 10(1), must indicate that the public body is unable to confirm or deny the existence of the requested records and that, if such records did exist, they would be excepted from disclosure under section 16 of the Act (disclosure harmful to public or individual safety). The response must also provide the contact information of someone who can answer questions about the decision and that the applicant can ask the Commissioner for a review.

A refusal to confirm or deny the existence of a record is a significant limit to the right of access. If an applicant asks the Information and Privacy Commissioner to review a refusal to confirm or deny the existence of a record, the public body will be required to provide detailed and convincing reasons why **section 10(2)** was applied.

Before refusing to confirm or deny the existence of a record, a public body is expected to determine whether or not any record exists in order to properly fulfil its duty to assist the applicant.

4.6 CONFIDENTIAL EVALUATIONS

Section 17 of the Act provides that a public body may refuse to disclose confidential evaluative information or opinions to an applicant in certain circumstances.

Section 17 is a discretionary exception and applies only when an individual, or a representative acting on their behalf, is requesting their own personal information. The exception applies to both the applicant's own personal information and the personal information of the individual supplying the evaluation or opinion.

The application of **section 17** is subject to a three-part test:

- The information must be evaluative or opinion material.
- It must be compiled for the purpose of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of contracts or other benefits.
- The information must be provided, explicitly or implicitly, in confidence.

This provision protects the process where information is compiled about an individual in order to assess their suitability for either employment or the awarding of contracts or other benefits. This may involve information on their personal strengths or weaknesses, or eligibility (fitness or entitlement), or qualifications (attainments and accomplishments).

The exception applies only to the selection process and not to evaluative processes relating to other aspects of employment or the awarding of contracts or benefits.

Employment refers to selection for a position as an *employee* of a public body, as defined in the Act (**section 1(c)**).

Contracts refers to agreements relating to both personal services and the supply of goods and services.

Other benefits refer to benefits conferred by a public body through an evaluative process. The term includes research grants, scholarships and prizes. It also includes appointments required for employment in a particular job or profession such as a special constable.

The term is not intended to refer to admission to programs of study, student or low-income housing, or benefits based solely on objective criteria.

For this exception to apply, the personal information must be contained in a confidential evaluation or opinion provided to the public body, but a summary of an evaluation that is compiled by the public body would also qualify.

Examples of such evaluations include:

- Verbatim transcription of a reference check of an employment candidate, supplied in confidence.
- A summary of a mix of telephone and written reference checks compiled by an official.

An analysis of the interview or of all reference checks prepared by the public body would not be excepted under this provision. Factual information such as statistics on absenteeism would also not be excepted.

Section 17(2) deals with the personal information of participants in a formal employee evaluation process concerning the applicant.

Participant is defined in **section 17(3)** as including a peer, subordinate or client of the applicant. It does not include the applicant's supervisor or superior.

Public bodies that incorporate "360 degree" evaluations into performance appraisals may withhold the names and positions of subordinates or colleagues, or the identity of students or clients of the applicant. In certain situations, such as those involving a very small review group, some or all of the evaluative comments may reasonably be expected to

reveal the identity of the reviewer and may be excepted.

Section 17(2) is not intended to allow the withholding of the evaluative or appraisal information itself.

For either **section 17(1)** or **section 17(2)** to apply, the information must be provided with either an explicit or implicit understanding that it will be held in confidence. This intention that confidentiality will be maintained may be explicitly stated in the record itself or in an agreement governing the process, or implied by the circumstances under which the information is submitted and received. Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality. It is not sufficient for the submitting party simply to stamp documents “Confidential.”

Public bodies are encouraged to have written policies dealing with the anonymity or absence thereof in such processes, and procedures in place to protect such anonymity.

Some factors that may be considered when determining whether information was received in confidence are set out in section 4.2 of this chapter.

4.7 DISCLOSURE HARMFUL TO LAW ENFORCEMENT

Section 18 of the Act deals with the application of exceptions to protect both law enforcement activities and information in certain law enforcement records. It contains a number of discretionary exceptions, and a mandatory exception requiring public bodies to refuse to disclose information if this would be an offence under an Act of Canada.

Law enforcement is defined in **section 1(e)** of the Act as:

- Policing, including criminal intelligence operations;
- A police, security or administrative investigation, including the complaint that gives rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred; or
- Proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the investigation are proceedings.

Policing refers to the activities of police services. It includes investigations of offences, prevention of crime, maintenance of law and order, security and protective services, and law enforcement research and analysis.

Criminal intelligence is information relating to a person or group of persons. It is compiled by police services to anticipate, prevent or monitor possible criminal activity.

Intelligence-gathering is sometimes a separate activity from the conduct of investigations. Intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, or to ensure the security of individuals or organizations.

Investigation refers to a systematic process of examination, inquiry and observation. It includes the complaint that leads to the investigation. The phrase *lead or could lead* indicates that investigations are part of law enforcement even if they do not actually result in proceedings in a court or tribunal.

A public body need not carry out the investigation for that investigation to meet the definition. The records must, however, be in the custody or control of a public body.

The definition includes the complaint that gives rise to an investigation. This means that the initial complaint receives the same consideration, if protection from disclosure is required, as the rest of the investigation.

The definition is, however, limited by the reference to a *penalty or sanction*.

A *penalty or sanction* would include a fine, imprisonment, revocation of a licence, an order to cease an activity, expulsion, or job loss.

A body other than the one carrying out the investigation can apply the penalty or sanction. This includes a body such as the RCMP or another federal agency that is not a public body as defined in the Act. Corporate security investigations can lead to a police investigation or to laying of charges.

To apply the law enforcement exception, public bodies will need to ensure that a specific authority to investigate is in place and that the investigation can lead to a penalty or sanction being imposed.

Three types of investigations are specifically included: police, security and administrative investigations.

A *police investigation* is one carried out by the police, or other persons who carry out a policing function that involves investigations. For example, a police investigation may include an investigation by a special constable appointed under the *Police Act*, or by an officer responsible for investigating possible offences under a federal or provincial enactment.

A *security investigation* includes an activity carried out by, for, or concerning a public body and relates to the security of the organization and its clients, staff, resources, or the public. Security includes the work that is done to secure, ensure safety or protect from danger, theft or damage. Examples include investigations of employee theft, unlawful access to computer systems, and trespass on public body property.

Investigations carried out by information technology staff as part of protecting the integrity of computer hardware and software may also be considered security investigations.

An *administrative investigation* is a formal investigation carried out to enforce compliance or to remedy non-compliance with standards, duties and responsibilities. These standards, duties and responsibilities may be defined under an Act or regulation. Examples include liquor licensing inspections under the *Liquor Control Act* and fire investigations under the *Fire Prevention Act*.

Because of the nature of administrative investigations, they may not always be specifically authorized in an Act or regulation. Standards, duties and responsibilities may be defined in a formal policy of the public body. The establishment of a policy demonstrates that the public body considers an issue to be of sufficient importance to warrant the use of investigative procedures and the establishment of a possible sanction or penalty. It also demonstrates endorsement of the procedure and sanction by the governing body or the head of the public body.

Such policies should be clear about:

- The authority for the investigation
- The nature of the investigation and procedures that must be followed
- The nature of the penalty or sanction

Examples of this type of investigation would include:

- An investigation in response to a complaint under a public body's sexual harassment policy; or
- An investigation in accordance with a public body's policy on maintaining confidentiality of client, staff and organizational information.

The regular day-to-day review and monitoring of employee performance, including employee grievances, would generally not be considered an administrative investigation that is defined as law enforcement.

A civil action for monetary damages or recovery of a debt, or an internal employment-related investigation where a tribunal could hear the matter only at the insistence of the

employee does not fall within this section.

Investigations performed under the authority of a federal or provincial Act or regulation which can result in a prosecution would generally be considered to be part of law enforcement. The specific facts of the matter would determine whether it was a police, security or administrative investigation.

Proceedings include an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions concerning a person's rights. This includes administrative proceedings before agencies, boards and tribunals that lead or could lead to a penalty or sanction being imposed, including a penalty or sanction imposed by another body to which the results of the proceeding may be referred.

Section 18(1) is a discretionary exception. It provides that a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to:

- Interfere with or harm a law enforcement matter including an ongoing or unsolved law enforcement matter;
- Prejudice the defence of Canada or of any foreign state allied to or associated with Canada, or harm the detection, prevention or suppression of espionage, sabotage or terrorism;
- Harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement;
- Reveal the identity of a confidential source of law enforcement information.
- Reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities;
- Reveal any information relating to prosecutorial discretion;
- Deprive a person of the right to a fair trial or impartial adjudication;
- Reveal a record that has been confiscated from a person by a peace officer in accordance with a law;
- Facilitate the escape from custody of an individual who is being lawfully detained;
- Facilitate the commission of an unlawful act or hamper the control of crime;
- Reveal technical information relating to weapons or potential weapons;
- Harm the security of any property or system, including a building, a vehicle, a computer system or a communications system; or
- Reveal information in a correctional record supplied, explicitly or implicitly, in confidence.

Interfere with or Harm a Law Enforcement Matter (section 18(1)(a))

This provision allows a public body to refuse to disclose information that could either

interfere with or harm a law enforcement matter, including an ongoing or unsolved law enforcement matter.

Interfere with includes hindering or hampering a law enforcement matter and anything that would detract from an investigator's ability to pursue the investigation.

Harm implies damage or detriment. The harm threshold is designed to protect law enforcement while preserving the public's right of access to some types of law enforcement information.

The exception includes ongoing or active investigations and proceedings and those where investigative activity has ceased but the crime remains unsolved. This includes investigations where no prosecution has resulted, but not those where charges were dropped.

An example would be an unsolved murder or a fraud investigation where there was insufficient evidence for prosecution at the time of the investigation.

The public body must demonstrate the harm that would result from disclosure or the way in which disclosure would interfere with or hinder the law enforcement matter. The likelihood of harm will depend, in part, on the sensitivity of the law enforcement information.

To invoke this exception, a public body must establish a direct link between the disclosure of specific law enforcement information and the harm that is expected to result from release. It cannot simply claim harm to law enforcement in general.

A public body does not need to demonstrate that actual harm will result or that actual harm resulted from similar disclosures in the past. However, past experience is a valuable indicator of the expected harm.

Prejudice to the Defence of Canada (section 18(1)(b))

This provision allows a public body to refuse disclosure of information that could reasonably be expected to be detrimental to national security.

Public bodies in Prince Edward Island hold only limited information related to national security. However, the presence of military installations within the province and the need for cooperation between the federal and provincial governments for emergency planning are matters that could fall within the scope of this exception.

Prejudice in this context refers to detriment to national security interests.

Defence of Canada means any activity or plan relating to the defence of Canada, including improvements in the nation's ability to resist attack.

An *allied state* is one with which Canada has concluded formal alliances or treaties. An *associated state* is one with which Canada may be linked for trade or other purposes outside the scope of a formal alliance.

This provision also permits the public body to refuse disclosure of information that would harm the detection, prevention or suppression of espionage, sabotage or terrorism. The test for *harm* in this part of the exception is more demanding than the test for *prejudice* required in the first part. There must be clear and convincing evidence that harm to the detection, prevention or suppression of espionage, sabotage or terrorism could occur if the requested information were disclosed.

Espionage is any activity carried out by spies, or activity related to spying.

Sabotage is malicious or wanton destruction, usually, but not always, directed against property.

Terrorism involves acts of serious violence and related activities that create fear in individuals, groups or nations and which are generally aimed at coercing government or communities into taking or ceasing specific actions.

Examples include information relating to industrial sabotage or terrorism and information concerning local security arrangements for a meeting of heads of state or an international sporting event.

Effectiveness of Investigative Techniques and Procedures (section 18(1)(c))

This provision permits a public body to refuse disclosure of information that could harm the effectiveness of investigative techniques used in law enforcement. It recognizes that unrestricted access to law enforcement techniques could reduce their usefulness, proficiency and success (ex., effectiveness).

Investigative techniques and procedures encompass the methods and processes by which examinations, inquiries and observations are carried out, and include the equipment and technology employed in these activities.

The harms test precludes the refusal of basic information about well-known investigative techniques such as wire-tapping, fingerprinting or standard sources of information about individuals' addresses, personal liabilities, real property, etc.

The focus in the exception is on the refusal of information that relates directly to the continued effectiveness of investigative techniques and procedures. Examples where less information might be disclosed are DNA testing or new technologies in electronic eavesdropping.

The exception extends to techniques and procedures *likely to be used*, in order to protect techniques and technology under development and new equipment or procedures that have not yet been used.

Identity of a Confidential Source (section 18(1)(d))

This provision enables a public body to refuse to disclose information that reveals the identity of a confidential source of law enforcement information.

The fact that the information, if disclosed, could reveal the identity of a confidential source is sufficient to apply this exception. There is no need to actually demonstrate that harm could come to the source.

Identity includes the name and any identifying characteristics, symbols and numbers relating to the source.

A *confidential source* is someone who supplies law enforcement information, as defined in the Act, to a public body on the assurance that their identity will remain secret. Employees, whether directly employed or under contract, cannot be *sources* because they are a part of a public body and are supplying information as part of their job.

Where a public body can demonstrate that the source is indeed confidential and is supplying law enforcement information, it then determines whether the particular information requested could possibly permit the applicant or anyone else to identify the source. Since it is often difficult to determine whether information can be linked to provide identification, caution should be exercised in releasing any information connected to a confidential source.

See also Police Informer Privilege in Chapter 4.14 of this publication. If police informer privilege applies, the information cannot be disclosed. This is a mandatory exception to disclosure because privileged information of a third party is involved (**section 25(2)**).

Reveal Criminal Intelligence (section 18(1)(e))

This provision allows a public body to refuse disclosure of information that could reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of:

- Organized criminal activities; or
- Serious and repetitive criminal activities

Criminal intelligence operations are related to policing activities but are mentioned separately to emphasize that they are covered in the exception.

Criminal intelligence is information relating to a person or group of persons compiled by law enforcement agencies to anticipate, prevent or monitor possible criminal activity. This exception does not require an expectation of harm. In order to qualify for this exception, the criminal intelligence must have a reasonable connection with operations relating to organized crime or with serious and repetitive criminal activities. A public body wishing to rely on this exception would have to be able to demonstrate a rational relationship between the information collected and the operations for which that information may be used.

Intelligence-gathering is often unrelated to the investigation of a specific offence. For example, intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, and for ensuring the security of individuals or organizations.

Intelligence may be drawn from investigations of previous incidents that may or may not have resulted in the trial and conviction of the person under surveillance.

Organized criminal activities occur when a group of people come together with the intent of committing crimes or when they conspire together to commit crimes. There is a degree of organization or deliberate planning involved, which is not the case with random criminal acts. Examples may include the activities of gangs and automobile theft rings, smuggling narcotics, and transporting illegal immigrants.

Serious and repetitive criminal activities occur when an individual, or group of individuals, commit the same crime repeatedly. The criminal activity has to be one that carries a heavy penalty or has major impact on society or individuals.

Examples include serial bank robberies, dealings in illegal drugs and ongoing industrial sabotage.

Prosecutorial Discretion (section 18(1)(e.1))

This provision allows a public body to refuse to disclose information related to the exercise of discretion by Crown Counsel with regard to prosecuting an offence.

This includes information on whether or not to:

- Approve a prosecution;
- Stay a proceeding;
- Prepare for a hearing or trial;
- Conduct a hearing or trial;
- Take a position on a sentence; or
- Initiate an appeal.

The exercise of this discretion applies to offences under the *Criminal Code* (Canada) and any other enactment of Canada for which the Attorney General for Prince Edward Island may initiate and conduct a prosecution. It also extends to offences under an enactment of Prince Edward Island, including prosecution of provincial regulatory offences. Most records relating to this exception will be in the custody or under the control the Attorney General's office. Copies of records or notes reflecting the discretion exercised may be in the files of other public bodies.

Section 18(1.1) states that this exception does not apply to information that has been in existence for 10 years or more. Normally this is determined by matching the day and month on the face of a record to the same day and month ten years later. Where the date is not obvious, it will be necessary to examine the context of the record, other documents that may be in proximity to it in a file and other facts that will help to provide a date.

Fair Trial or Impartial Adjudication (section 18(1)(f))

This provision enables a public body to refuse to disclose information that could reasonably be expected to deprive a person of the right to a fair trial or impartial adjudication. The exception applies to a person. *Person* includes an individual, a corporation, a partnership and the legal representatives of a person.

Fair trial refers to a hearing by an impartial and disinterested tribunal that renders judgment only after consideration of the evidence and the facts.

Impartial adjudication means a proceeding in which the parties' legal rights are safeguarded and respected.

It is important that discussions proceed and decisions on these matters continue to be made in a candid manner without any fear of interference from outside influences.

This exception applies beyond law enforcement and civil and criminal court actions to proceedings before tribunals established to adjudicate individual and collective rights. Examples include hearings before the Island Regulatory and Appeals Commission and the

hearings of a human rights panel.

In applying the exception, the public body must present specific arguments about how and why disclosure of information could deprive a person of the right to a fair trial or hearing. Commencement of a legal action is not by itself enough to support application of this exception.

An example of a case where the exception might apply would be if there were a request for information about alleged sexual abuse collected as part of a case against an individual. Disclosure of such information before legal proceedings were completed could reasonably be expected to detract from an individual's right to a fair trial.

Confiscated Records (section 18(1)(g))

This provision permits a public body to refuse disclosure that would reveal a record that has been seized from a person by a peace officer in accordance with the law. The provision covers individuals, corporations and partnerships, and their representatives.

A *peace officer* includes a mayor, sheriff or sheriff's officer, warden, correctional officer, and any other officer or employee of a penitentiary, prison or correctional centre. It also includes a police officer, police constable or other person employed for the preservation or maintenance of public peace.

The record must have been confiscated under the authority of a law or statute. An example would be business records of a company under investigation for suspected tax fraud where its records have been seized.

Facilitating Escape from Custody (section 18(1)(h))

This provision allows a public body to refuse disclosure of information where release could reasonably be expected to facilitate the escape from custody of a person who is lawfully detained.

Lawfully detained means being held in custody pursuant to a valid warrant or other authorized order. This would include:

- Those in custody under federal or provincial statute.
- Young persons in open or secure custody or pre-trial detention under the Prince Edward Island *Young Offenders Act*.
- Those involuntarily committed to psychiatric institutions.
- Parole violators held under a warrant.

The exception also extends to individuals remanded in custody (ex., charged but not yet found guilty and sentenced). It does not apply to individuals released under bail supervision. An example of information protected by this exception is the building plans for a correctional facility.

Facilitate the Commission of an Unlawful Act (section 18(1)(I))

This provision permits a public body to refuse to disclose information that would be of use in committing a crime or that could hamper the control of crime. Examples include information about techniques, tools and instruments used for criminal acts, names of individuals with permits for guns, the location of police officers, and the location of valuable assets belonging to a public body.

Reveal Technical Information Relating to Weapons (section 18(1)(j))

This provision enables a public body to refuse the disclosure of information that could reasonably be expected to make the applicant or others aware of technical information relating to weapons or to materials that have the potential to become weapons. This exception would cover information such as how to make a bomb.

Security of Property and Systems (section 18(1)(k))

This provision permits the public body to refuse to disclose information that could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system, and a communications system. The same rules for determining harm apply as to other parts of **section 18** where there is a harms test.

Security generally means a state of safety or physical integrity. The security of a building includes the safety of its inhabitants or occupants when they are present in it. Examples of information relating to security include methods of transporting or collecting cash in a transit system, plans for security systems in a building, patrol timetables or patterns or security personnel, or the access control mechanisms and configuration of a computer system.

Correctional Record (section 18(1)(l))

This provision enables a public body to refuse to disclose all or part of a record that could reasonably be expected to reveal information in a correctional record supplied explicitly or implicitly in confidence.

A *correctional record* refers to information collected or compiled while an individual, either an adult or young person, is in the custody or under the supervision of correctional

authorities or their agents as a result of legally imposed restrictions. It includes records relating to:

- Imprisonment
- Parole
- Probation
- Community service orders
- Bail supervision
- Temporary absence permits

The record itself need not be in the custody or control of the public body. It will suffice if the information would reveal information that is in the correctional record. The information may be an extract from the record or a summary of the record.

To qualify for the exception, the information must have been supplied in confidence. This means that there is an agreement or understanding between the parties or some long-standing practice governing how the information will be treated. This may be explicit, in that it has been agreed to in writing, or implicit, in that both parties assume the confidentiality.

It is not sufficient to simply mark the information as being received in confidence. There must be evidence that a condition of confidentiality is a normal part of the process of supplying the information. For more information on the confidentiality, see **section 4.3** of this chapter.

Section 18(2) is also a discretionary exception. It allows non-disclosure of information that could expose an individual to civil liability or could harm the proper custody or supervision of an individual under correctional supervision.

Exposure to Civil Liability (section 18(2)(a))

Section 18(2)(a) allows a public body to refuse to disclose information to an applicant if the information is in a law enforcement record and the disclosure could reasonably be expected to expose an individual to civil liability. To qualify for this exception, the individual must either be the author of the record, or be quoted or paraphrased in the record. This exception protects law enforcement officials, and those providing information to them, from civil suit as a result of disclosure of records made while carrying out law enforcement activities.

Individual under the Supervision of Correctional Authority (section 18(2)(b))

Section 18(2)(b) allows a public body to refuse disclosure of information about the history, supervision or release of a person who is in custody or under the supervision of a correctional authority. The exception applies only if disclosure could reasonably be expected to harm the proper custody or supervision of that person. The same harms test is required as for **section 18(1)(a)**.

History means information about the person such as an employment record or medical information.

Supervision refers to the overseeing of a person.

The provision applies to adults and young persons still subject to control by correctional authorities or their agents as a result of legally imposed restrictions on their liberty.

This includes individuals in prison, on parole, on probation, on a temporary absence permit, under bail supervision or performing community service work. The exception allows discretion to except specific information about someone in custody or under supervision. Examples include security arrangements for the transfer of a prisoner between facilities, whether or not a prisoner is in a public hospital, and the appointment of a probation officer. This exception cannot be used to deny access to an applicant who is no longer in custody and is seeking their own personal information.

Offence under Act of Canada (section 18(3))

Section 18(3) is a mandatory exception. It provides that a public body must refuse to disclose information to an applicant if the information is a law enforcement record and the disclosure would be an offence under an Act of Canada.

Law enforcement record means any recorded information relating to law enforcement as defined in the *Act*.

An offence under an Act of Canada means a breach of a federal statute. It excludes lesser instruments such as federal regulations, orders or rules. Examples of such legislation are:

- The *Young Offenders Act* (Canada), where it is an offence to knowingly disclose certain court, police, government and other records relating to young offenders except as authorized by that Act.
- The *Official Secrets Act* (Canada), which prohibits disclosure of information that could prejudice the security of the country.
- The *Criminal Code* (Canada), which prohibits the release of wiretap transcripts.

When the Exception Does Not Apply (section 18(4))

Section 18(4) of the Act provides that **section 18(1)** and **section 18(2)** do not apply to:

- A report prepared in the course of routine inspections by an agency that is authorized to enforce compliance with an Act of Prince Edward Island (**section 18(4)(a)**).
- A report, including statistical analysis, on the degree of success achieved in a law enforcement program, unless disclosure of the report could reasonably be expected to interfere with or harm the matters referred to in **section 18(1)** or **(2)**.

The intent is to encourage disclosure of reports and statistics about law enforcement programs.

Routine inspections involve periodic visits by public officials to ensure that standards or other criteria are being met. They take place without specific allegations or complaints having been made. Examples include public health inspections, fire inspections, liquor licensing inspections, and safety inspections on vehicles. Such reports are usually factual in nature and report the conditions found by the inspector. They may include advice or other information that could be excepted under other sections of the Act.

Reports and statistics on the success of law enforcement programs should also be routinely disclosed whenever possible. Only if the contents of the report could interfere with or harm any of the matters set out in the preceding sections would information be withheld, and this would be done by severing the appropriate parts of the report. Examples include information on programs such as “Crime Stoppers” statistics on elevator safety inspections, and reports on matters such as success in preventing abuse of handicapped parking stalls.

Completed Investigations (section 18(5))

Section 18(5) of the Act provides that, after a police investigation is completed, a public body may disclose the reasons for the decision not to prosecute:

- To a person who knew of and was significantly interested in the investigation, including a victim or a relative or friend of a victim (**section 18(5)(a)**).
- To any other member of the public, if the fact of the investigation was made public (**section 18(5)(b)**).

This disclosure would be in response to a request for access to information under the Act. Disclosure of the decision not to prosecute is permitted only to persons who knew of *and* were significantly interested in the investigation, unless the fact of the investigation itself is public knowledge.

There is no general requirement to release information about decisions not to prosecute unless the investigation itself was made public. To apply **section 18(5)(b)** there would have to be evidence of this fact, such as a newspaper report about the investigation or a news release.

The provision relates only to police investigations and not to the whole field of law enforcement.

Existence of Record

There are situations in which the disclosure of the mere existence of a record could result in harm to law enforcement. For example, disclosure of the existence of investigation records or criminal intelligence may indicate that enforcement activities are being undertaken and this, in itself, could harm those activities.

Section 10(2)(a) of the Act provides that a public body may, in response to an applicant, refuse to confirm or deny the existence of a record containing information described in **section 18**.

When the existence of a record is neither confirmed nor denied, the response to the applicant, as required under section 10(1), must indicate that the public body is unable to confirm or deny the existence of the requested records and that, if such records did exist, they would be excepted from disclosure under section 18 of the Act (disclosure harmful to law enforcement). The response must also provide the contact information of someone who can answer questions about the decision and that the applicant can ask the Commissioner for a review.

The same conditions apply as outlined in **section 4.4** of this chapter.

4.8 INTERGOVERNMENTAL RELATIONS

Section 19 provides that a public body may refuse to disclose information that could harm intergovernmental relations or the intergovernmental supply of information.

Section 19 is a discretionary exception.

Section 19(1) allows a public body to refuse access if disclosure could reasonably be expected to:

- Harm relations between the Government of Prince Edward Island or its agencies and any of the following or their agencies:
 - The Government of Canada or a province or territory of Canada;
 - **A municipality**

- The government of a foreign state; or
 - An international organization of states;
- or
- Reveal information supplied explicitly or implicitly in confidence by a government or an organization listed above or its agencies

This exception has two parts, one dealing with *harm to relations* and the other with *information given in confidence*.

Harm to Relations (section 19(1)(a))

This provision applies to information the disclosure of which could reasonably be expected to harm relations between the Government of Prince Edward Island and the listed external government entities (**includes municipalities effective June 12, 2018**). It includes both current and future relations.

Relations is intended to cover both formal negotiations and more general exchanges and associations between the Government of Prince Edward Island and other governments and their agencies.

Harm means damage or detriment to negotiations and general associations and exchanges. The threshold of harm is relatively high. To satisfy the test there must be more substantial grounds than fear that disclosure would merely hinder, impede or minimally interfere with the conduct of intergovernmental relations or negotiations.

The term *Government of Prince Edward Island* connotes a broader sense here than that of an individual public body. The exception has a different and higher-level coverage, in that *government* is intended to convey the sovereign power of the state in carrying out its will and functions. The exception is available only where disclosure of information could harm the conduct of intergovernmental relations of the province as a government entity, as opposed to interdepartmental relations.

Public bodies wishing to invoke **section 19(1)(a)** must demonstrate that the conduct of intergovernmental relations of the Government of Prince Edward Island, and not just those of the public body, would be harmed by disclosure. The exception relates to government bodies external to the Government of Prince Edward Island. It also covers any of their agencies (i.e., corporate bodies or persons designated by any of the listed external government organizations). For example, the Department of National Defence is an agency of the Government of Canada and UNESCO is an agency of the United Nations.

The provision covers not only *provincial governments* but also *territorial governments* (e.g., the Government of the Yukon) and their agencies.

A *foreign state* refers to the government of any foreign nation or state, including the component state governments of federated states.

An *international organization of states* refers to any organization with members representing and acting under the authority of the governments of two or more states. Examples would be the United Nations or the International Monetary Fund.

An example of information that might qualify for this exemption is correspondence between the Department of Health and Social Services and Health Canada regarding health funding, where disclosure might severely damage the ability of the Government of Prince Edward Island and this national body to carry on negotiations.

Disclosure of Information

Section 19(2) of the Act stipulates that information referred to in **section 19 (1)(a)** may only be disclosed with the consent of the Minister responsible for the FOIPP Act (i.e., the Attorney General) in consultation with the Executive Council.

Where a public body wishes to disclose information that qualifies for the exception set out in **section 19 (1)(a)**, it must prepare a submission describing the information and setting out the circumstances and reasons why it wishes to disclose this information. The submission should be prepared in consultation with the Intergovernmental Affairs Division of the Executive Council Office and with the other government, as appropriate. This submission must then be signed by the head of the public body and submitted to the Attorney General for consideration. If, after discussion of the matter with the public body and with other appropriate departments, the Attorney General believes that disclosure should take place, the Attorney General and the head of the relevant Prince Edward Island Government department will jointly sponsor the submission to the Executive Council for consultation. After this consultation, the Attorney General will either consent to, or deny, the application.

Information Received In Confidence (section 19(1)(b))

This section provides protection for information that could reasonably be expected to reveal information received in confidence from one of the bodies specified in **section 19(1)(a)**.

A decision that a confidence would be revealed is enough to satisfy the test here. It is *not* necessary that the harms test set out in **section 19 (1)(a)** also be met.

In order to be covered by **section 19(1)(b)**, the information must have been supplied in circumstances that clearly place an obligation on the public body to maintain confidentiality.

In confidence usually describes a situation of mutual trust in which private matters are related or reported.

Criteria for determining whether information has been given *in confidence* are provided in **section 4.3** of this chapter.

The burden of determining that information was submitted *in confidence* lies with the public body.

The intention to maintain confidentiality may be explicitly stated within the record itself, or in an agreement between the parties, or may be implied by the circumstances under which the information was submitted and received.

Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality. It is not sufficient for an external governmental entity to stamp documents “Confidential” or to assert that the information was supplied in confidence, although this will assist in the determination. There must be evidence to support the assertion and to prove that the information has been treated consistently in a confidential manner.

Examples of information that may be supplied in confidence include:

- Correspondence about and transcripts of a confidential meeting of the Maritime Premiers.
- Negotiating strategies relating to a federal, provincial and municipal infrastructure program.

Consent to disclose: **Section 19(3)** of the Act provides that a public body may disclose information supplied in confidence only with the consent of the government (provincial, territorial or foreign), the organization or the agency that supplied the information.

Consultation with the other party or parties providing the information should take place between officials who are authorized to make decisions about disclosure. The consent of the government, organization or agency that provided the information should be in writing.

Limitation on Section 19 (section 19(4))

This provision states that **section 19** does not apply to information that has been in existence in a record for **15** years or more. Normally, this is determined by matching the day and month on the face of a record to the same day and month **15** years later. Where the date is not obvious, it will be necessary to examine the context of the record, other documents that may be in proximity to it in a file and other facts that will help provide a date. Information qualifying for exception under **section 19** but which is 15 more years old must be released unless another exception applies to it.

Consultation

Consultations regarding whether or not to invoke this exception should normally take place between the FOIPP Analyst of the public body and officials in comparable positions in external government bodies. Where the federal or foreign governments or international organizations are involved, consultations must be conducted in cooperation with the Intergovernmental Affairs Division of the Executive Council Office. Public bodies that will need to consult on a regular basis should establish practices and contact points to expedite the process.

4.9 CABINET CONFIDENCES

Section 20(1) creates a mandatory exception for information that would reveal the substance of deliberations of the Executive Council or any of its committees. The exception applies to any advice, recommendations, policy considerations or draft legislation or regulations submitted to or prepared for submission to these bodies.

Section 20(1) is intended to preserve the unique role of Cabinet institutions and conventions within the framework of parliamentary government in Prince Edward Island. This is based on the convention of collective ministerial responsibility to the Legislature and the people of the province for the actions of the government.

In practice, all members of a Cabinet are expected to publicly support the government's actions and policies. In order to facilitate this collective decision-making, Cabinet discussions and deliberations have traditionally been kept confidential. This permits full and frank discussions around the Cabinet table. Ongoing confidentiality is required in order to avoid breaking a position of unity once a decision has been made.

In addition, there are situations where Cabinet may wish to delay public announcement of its decisions. It may have entered into arrangements with other governments or with affected individuals to postpone an announcement of a decision until a specific time.

Cabinet may also develop plans to deal with issues, emergencies or contingencies. The value of these plans would be diminished if immediate access were granted to its decision-making processes.

Standing Policy Committees (SPCs) are not considered Cabinet committees. It is recognized that information often flows between Cabinet and SPCs and it is often difficult to distinguish the origins and purpose of particular information. In dealing with SPC records, or records created for SPCs, **sections 20, 22** (advice and recommendations) and **4(1)(i)** (which excludes some SPC information from the scope of the Act) must be applied in concert with each other.

Because **section 20** deals with the Cabinet process, the Office of the Executive Council makes all decisions relating to submissions to the Executive Council and related records (ex., minutes and agendas).

Departmental decisions on disclosure of other records that include reference to Cabinet confidences are subject to approval by the Office of the Executive Council. Consultation on confidences of the Executive Council must be conducted through the FOIPP Analyst for the Office of the Executive Council.

Substance of Deliberations

In considering this exception, it is important to determine whether or not a record or part of a record reveals the substance of the deliberations of the Executive Council or any of its committees, either explicitly or implicitly.

A release of information *explicitly* reveals the substance of deliberations if the information itself contains the essence of the discussion or deliberations or reveals the contents of the deliberations.

A release of information *implicitly* reveals this type of information if it is reasonable to expect that disclosed information could be combined with other information to reveal the substance of Executive Council or committee deliberations.

In this provision, *substance* means the essence or essential part of a deliberation.

Deliberation means the act of weighing and examining the reasons for and against a contemplated act or course of conduct. It also includes an examination of choices of direction or means to accomplish an objective.

Meaning of Executive Council

The Executive Council is commonly known as the provincial Cabinet and refers to a group of ministers acting collectively. **Section 20(1)** does not apply to a minister acting alone, unless the individual minister is carrying out the direction of Cabinet or is acting as a Cabinet committee.

Committees of the Executive Council include:

- **Treasury Board**
- **Operations Committee**
- **Policy Board**

Examples of Records

Examples of records that would reveal the substance of deliberations of the Executive Council or one of its committees are:

- Agendas, minutes and related documents of Executive Council meetings.
- Letters and memoranda concerning issues deliberated upon or the decisions or directions taken by ministers but not made public – these may have been sent to ministerial colleagues or senior public servants.
- Briefing material placed before Executive Council or one of its committees.
- A memorandum (including electronic mail) from the Clerk of Executive Council to ministers discussing Cabinet decisions.
- A memorandum (including electronic mail) from a deputy minister to an assistant deputy minister or chief executive officer or other senior officer dealing with issues that will be or have been deliberated upon by the Executive Council or one of its committees.
- A record of discussions between senior officials about issues that will be or have been deliberated upon by the Executive Council or one of its committees.
- A briefing note from a deputy minister or chief executive officer to a minister concerning what will be, is or has been discussed in Executive Council or one of its committees.
- A draft or final submission to Executive Council.

The listing of types of records included in **section 20(1)** (advice, recommendations, policy considerations, and draft legislation or regulations) is illustrative only. These are simply examples of certain types of information likely to reveal deliberations of the Executive Council or its committees.

Advice, recommendations refers to the substance of a suggested course of action which is the subject of deliberation. Advice is analysis and presentation of various options and not the presentation of fact. To qualify for this exception it must deal with issues that will be, are or have been discussed by the Executive Council or one of its committees.

Policy considerations refers to analysis and flagging of issues that deserve special consideration by Ministers when taking action or deciding policy at Executive Council or a committee.

Draft legislation or regulations refers to versions of bills intended to become Acts or of legislative instruments intended to be enacted under the authority of an Act or the authority of the Lieutenant Governor in Council. This provision relates to draft legislation or regulations discussed by ministers.

When the Exception Does Not Apply

Section 20(2) sets out two circumstances where **section 20(1)** does not apply.

Information in a record that has been in existence for 15 years or more (section 20(2)(a))

The exception in **section 20(1)** applies only to records or portions of records that have been in existence less than **15** years. Other exceptions may apply to particular information in these records. **15** years means the period from a particular month and day to a corresponding month and day **15** years later.

Information in a Record of a Decision made by the Executive Council or any of its Committees on an Appeal under an Act (section 20(2)(b))

Where the Executive Council or one of its committees functions as an appeal body under an Act and makes a decision, the decision and any recorded reasons for the decision are available to the public. Other portions of the record, such as the advice and recommendations supporting the deliberative process leading to a decision, remain subject to **section 20(1)**.

4.10 PUBLIC BODY CONFIDENCES

Section 21(1) of the Act provides that a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to reveal information to an applicant such as:

- a draft of a resolution, bylaw or other legal instrument by which the public body acts;
- or where an enactment authorizes a meeting of the officials or governing body of a public body or a committee of the governing body of the public body to be held in the absence of the public, if the disclosure could reasonably be expected to reveal the substance of deliberations of the meeting.

Section 21 is a discretionary exception. The **provision refers to information, not records**, which means that the exception should be applied only to that portion of a record containing information covered by this provision. The remainder of the severed record would be disclosed to the applicant unless another exception was invoked.

For example, an applicant requests a copy of a memorandum sent by the chair of a committee of a board to committee members. The memorandum discusses a number of administrative matters and also discusses an issue that the committee must discuss at a forthcoming meeting that will not be open to the public. The information relating to this latter issue may be severed from the record if it would reveal the substance of deliberations of the committee on a matter specified in an enactment as one that may be considered *in camera*. The applicant would receive the remainder of the record unless other exceptions applied to it.

Draft Resolution, By-law or Other Legal Instrument

Draft means a version of the resolution, by-law or other legal instrument that has not been finalized for consideration in public by the public body. The exception can apply to the whole draft record or to individual sections or clauses.

A *resolution* means a formal expression of opinion or will of an official body or public assembly, adopted by a vote of those present. The term is usually employed to denote the adoption of a motion such as an expression of opinion, a change to rules or a vote of support or censure.

A *by-law* means a rule adopted by a public body with by-law making powers. The intent of this provision is to extend to all legal instruments of a public body the same protection extended to provincial legislation and regulations in **section 22(1)(e)**. Drafts are protected; the final version of the by-law, resolution or policy is not.

Substance of Deliberations of *In Camera* Meetings

In **section 21(1)(b)**, *substance* means the essence or essential part of discussion or deliberation.

Deliberation means the act of weighing and examining the reasons for and against a contemplated act or course of conduct. It also includes an examination of choices of direction or means to accomplish an objective.

Meeting means an assembly or gathering at which the business of the public body is considered. It includes both the meeting in its entirety and a portion of a meeting.

Governing body means the assembly of persons who are responsible for the administration of the public body.

Committee of its governing body means a group of people who have been designated by the governing body of the public body to act on its behalf and consider a particular issue or subject. A committee may be composed of elected officials, members of the public body or other persons designated to act by the public body.

In order for information relating to a meeting held *in camera* to qualify for this exception, the holding of the meeting in the absence of the public must be authorized by a Prince Edward Island Act or regulation, including the FOIPP Regulations.

A public body must rely on an authority as described above to authorize a meeting in the absence of the public and have grounds for excepting the substance of deliberations of such a meeting.

In the absence of the public means in the absence of the public at large. A meeting may still be considered to be held in the absence of the public if it is attended by a member of a

public body who is not an official, member of the governing body or member of a committee of the governing body.

A meeting open to the public, which no members of the public happen to attend, is not a meeting held in the absence of the public.

A meeting that is permitted to be held *in camera*, but to which the public is nevertheless invited, is also not a meeting held in the absence of the public.

However, a meeting, which may be held *in camera*, but to which certain members of the public are specifically invited to discuss sensitive issues pertaining to their property or themselves or their rights, is a meeting held in the absence of the public.

Common types of records relating to *in camera* meetings that may be protected are agendas, minutes, personal notes, and other records that document the substance of deliberations within such a meeting.

Actual documents that may be the subject of discussions could not normally be withheld under this section. However, the substance of deliberations about such documents may be withheld. This information will usually be part of other records and will have to be severed from them.

When the Exception Does Not Apply

The exception in **section 21(1)(a)** does not apply where the draft of the resolution, by-law or policy has been considered in a meeting open to the public. This means that, if a particular draft is discussed in a public meeting, there is no reason to deal with the information under an exception. Prior or subsequent drafts that are not considered in a public meeting can still be protected.

The exception in **section 21(1)(b)** does not apply where the subject matter of the deliberation has been considered in a meeting open to the public. This means that, where a public body has not explicitly excluded the public from the meeting, the exception cannot be applied.

Finally, the exception cannot be applied to any information referred to in **section 21(1)(a)** and **(b)** if it is in a record that has been in existence for **15** years or more. **15 years** means the period from a particular month and day to a corresponding month and day **15** years later. Other exceptions may still apply to the information.

4.11 ADVICE FROM OFFICIALS

Section 22(1) provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to reveal:

- Consultations or deliberations involving:
 - Officers or employees of a public body;
 - A member of the Executive Council; or
 - The staff of a member of the Executive Council (**section 22(1)(a)**).
- Positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the Government of Prince Edward Island or a public body, or considerations that relate to those negotiations (**section 22(1)(b)**);
- Plans relating to the management of personnel or the administration of a public body that have yet to be implemented (**section 22(1)(c)**);
- The contents of draft legislation, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council (**section 22(1)(d)**);
- The contents of agendas or minutes of meetings of an agency, board, commission, corporation, office or other body that is designated as a public body in the FOIPP Regulations (**section 22(1)(e)**);
- Information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision (**section 22(1)(f)**);
- Advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council (**section 22(1)(g)**); or
- The contents of a formal research or audit report that is incomplete unless no progress has been made on the report for at least 3 years (**section 22(1)(h)**).

Section 22(1) is a discretionary exception that is intended to protect the deliberative process involving senior officials and heads of public bodies, and their staff, as well as among officials themselves. It also protects the deliberative process involving senior officials, heads of public bodies and the governing authorities of public bodies.

The need for confidentiality in relation to various aspects of decision-making is not restricted to decisions by the Executive Council or the governing authorities of public bodies. An absolute rule permitting public access to all records relating to policy formulation and decision-making processes in public bodies would impair the ability of such bodies to discharge their responsibilities in a manner consistent with the public interest.

The exception is intended to provide a “deliberative space” for those involved in providing advice, carrying on consultations and making recommendations, so that records may be written with candor and cover all options. This “deliberative space” is especially important for those involved in the policy-making process. There is a need to preserve the relationships between senior officials and those advising them as part of the overall accountability of public organizations.

Senior officials and heads of public bodies may accept or reject the advice and recommendations of those advising them and they carry the responsibility of defending that decision.

The whole exception is discretionary in nature. Discretion is exercised in determining whether or not disclosure of a particular record or part of a record could reasonably be expected to reveal particular information about *either the process itself or the matters being discussed*.

In determining whether or not to invoke the exception, public bodies should undertake a three-step process.

They should:

- Determine whether the information requested falls within one of the classes of information to which the exception to disclosure may apply.
- If it does, then determine whether or not disclosure of the information can reasonably be expected to *reveal* the particular class of information involved.
- Exercise discretion as to whether or not to disclose the record or part of the record based on whether or not disclosure would affect similar advisory processes in the future.

The exercise of discretion regarding this type of advisory information should be based on the impact the disclosure can reasonably be expected to have on the public body's ability to carry out similar internal decision-making processes in the future.

Consideration should be given to whether disclosure of the information in this instance would:

- Make advisory processes less candid and comprehensive;
- Make consultations or deliberations less frank;
- Hamper the policy-making process;
- Destroy the ability of a public body or the government to develop and maintain strategies and tactics for present or future negotiations; or
- Undermine the public body's ability to undertake personnel or administrative planning.

Such determinations can only be made on a case-by-case basis, bearing in mind the magnitude of the process involved, the procedures for decision-making that have been followed, and the sensitivity of the particular information.

Public bodies should take into account the effect disclosure would have on all steps of a decision-making process and not just the immediate interests regarding the particular information in question.

The test for the exception is met if deliberative information is explicitly revealed or if a record makes direct reference to the deliberative processes.

As well, release of information can reveal deliberative processes implicitly if it allows an accurate inference to be made about those processes.

Eight specific areas meriting consideration for protection are set out in the Act. Each of these is discussed in detail below.

Consultations or Deliberations (section 22(1)(a))

This section allows discretion to refuse access to those records or parts of records containing *consultations or deliberations* involving officers or employees of a public body, a minister or a minister's staff.

A *deliberation* is a discussion or consideration by a group of individuals of the reasons for and against a measure.

A *consultation* is a very similar activity where the views of one or more individuals are sought about the appropriateness of particular proposals or suggested actions.

This discretionary exception is provided for the purpose of permitting the frank exchange of views among a number of individuals whose employment responsibilities include a consultative function.

Within public bodies, consultations and deliberations are normally carried on in an organized manner through the exchange of memoranda and proposals.

Agendas and minutes of meetings are also typical documents that may reveal consultations and deliberations. There is no blanket coverage for such records, but consultative and deliberative material may be severed from records of this nature.

The provision covers consultations or deliberations at all levels in a public body and also those involving a minister or their staff.

Positions, Plans, Procedures, Criteria or Instructions Developed for the Purpose of Contractual or Other Negotiations (section 22(1)(b))

This discretionary exception covers the strategies, plans, approaches and bargaining positions that have been employed or are contemplated for the purposes of contractual and other negotiations. It applies to individual public bodies and to the provincial government as a whole. Access to such information can be refused even after particular negotiations have been completed.

Positions and plans refer to information that may be used in the course of negotiations.

Procedures, criteria, instructions and considerations are much broader in scope, covering information relating to the factors involved in developing a particular negotiating position or plan.

Examples of the type of information that could be covered by this exception are the various positions developed by government or public body negotiators for the purpose of bargaining in relation to labour, financial and commercial contracts.

The exception extends to situations where an agent retained for these purposes carries out negotiations on behalf of the government or a public body.

Plans Relating to the Management of Personnel or Administration of the Public Body (section 22(1)c)

This provision covers plans relating to the internal management of public bodies, including information about the relocation or reorganization of government departments and agencies, as well as reorganization within public bodies.

The provision applies only within a limited time frame. Once a plan has been put into operation, the information relating to it can no longer be protected under this exception.

Management of personnel comprises all aspects of the management of human resources of a public body. This includes staffing requirements, job classification, recruitment and selection, employee salary and benefits, hours and conditions of work, leave management, performance review, training, separation and layoff. It also includes the management of personal service contracts.

Administration of a public body comprises all aspects of a public body's internal management, other than personnel management, that are necessary to support the delivery of programs and services. Administration includes business planning, and financial, materiel, contracts, property, information, and risk management.

Although the final plan must be released, the options that were considered before deciding on the plan need not be disclosed. Plans that are never implemented can be protected for 15 years, if there is reason to believe that injury or harm to the efficiency of the operation of the public body could reasonably be expected to result from disclosure.

Implementation means the point when the implementation of a decision begins. For example, a public body decides to go forward with an internal budget cut or restructuring of departments. Implementation commences when this plan of action is communicated to its organizational units.

Contents of Draft Legislation, Regulations and Orders (section 22(1)(d))

This provision covers bills, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council prior to publication, while they are being drafted and formulated in preparation for presentation to the Legislature, publication or public consultation. This provision covers all the drafts and not just the final draft of legislation, regulations and ministerial orders.

For draft by-laws and policies of public bodies, see section 4.10 of this chapter.

Contents of Agendas or Minutes of Meetings of the Governing Body of an Agency, Board, Commission, Corporation, Office or Other Body that is a Public Body (section 22(1)(e))

This exception applies only to those public bodies listed in **Schedule 1** of the FOIPP Regulations.

The provision establishes agendas and minutes of meetings as classes of record that can be protected because the meetings to which they relate provide the focus for decision-making within these types of bodies. The exception can be applied only to the records of the governing body or a committee of the governing body of the organization.

The exception covers only agendas and minutes of meetings, and not the background reports or studies used in a meeting. Background information must be released unless another exception applies.

Pending Policy and Budgetary Decisions (section 22(1)(f))

This provision covers information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision. It provides protection from premature disclosure of a policy or budgetary decision.

Once a policy or budgetary decision has been taken and is being implemented, the information can no longer be protected under this provision. A decision is being implemented once those expected to carry out the activity have been authorized and instructed to do so.

Advice and Recommendations

Section 22(1)(g) is intended to protect candor in the giving of advice and formulation of proposals, analyses, policy options, recommendations, and related alternatives for potential courses of action.

It covers such advisory functions at all levels in a public body. It also applies to advice and recommendations obtained from outside the public body, including those received under a contractual or other advisory arrangement. The exception provides specific coverage for advice, proposals, recommendations, analyses, and policy options developed by or for a member of the Executive Council.

There is some overlap between the terms *advice* and *recommendations* as used in the exception.

The term *recommendations* refers to formal recommendations about courses of action to be followed which are usually specific in nature and are proposed mainly in connection with a particular decision being taken.

Advice, on the other hand, refers to less formal suggestions about particular approaches to take or courses of action to follow.

Proposals and *analyses or policy options* are closely related to advice and recommendations and refer to the concise setting out of the advantages and disadvantages of particular courses of actions.

Former PEI Commissioner Judith Haldemann provides insight into the purpose of the exception under section 22 of the FOIPP Act in Order No. FI-10-005, Prince Edward Island (Department of Education and Early Childhood Development) (Re), 2010 CanLII 97256 (PE IPC). Commencing at page 13, she states:

“... One aspect of the business of government is the development of policies and procedures for a variety of matters that may result in heated criticism by the media and members of the public, as well as politicians. There are some aspects of governing which require an assurance that a decision maker may rely on their advisors and may require those advisors to develop and discuss various policy options that may be available to carry out a particular task that government has set itself. I agree with the Public Body that in order to carry out its policy work . . . effectively, the decision maker must be able to consult, deliberate, receive advice and analysis and other matters described in subsection 22(1) before coming to the final decisions on the issue. On the one hand, the public has a right to know what government is doing with the taxpayers’ money or what decisions are being made on the public’s behalf; on the other hand, a public body has to have working room to study and analyze the various issues before it reaches and announces its decision.”

The PEI Information and Privacy Commissioner in **Order No. FI-18-001, Public Schools Branch**, affirms Alberta Information and Privacy Commissioner’s criteria for *advice* are that it should be:

- Sought or expected, or be part of the responsibility of a person by virtue of that person’s position.
- Directed toward taking an action, including making a decision.

- Made to someone who can take or implement the action.

The Alberta Commissioner has determined that a statement of fact that is not directed toward action to be taken does not qualify as advice under this provision of **section 22**.

If the factual information is sufficiently interwoven with other advice that it cannot reasonably be considered separate or distinct, it qualifies under this exception.

Section 22(1)(g) would not normally apply to the details of a study or background paper where factual information is presented to describe certain issues, problems or events. Rather, it applies to the information used to formulate possible directions in dealing with an issue or problem, to establish a policy or to make a decision.

The nature and significance of many issues are such that disclosure of advice relating to them could reveal information that would cause great damage to the internal processes of decision-making in a public body. Disclosure could also affect its overall ability to effectively manage programs and activities.

It is equally true that there are other issues where more openness surrounding the advisory and decision-making process can be of benefit. There are also issues and activities of lesser significance where the disclosure of advice would have little or no effect on the overall administration or operation of the program or activity.

This section is intended to provide a zone of confidentiality around the policy-making process, rather than protecting all forms of advice. The public body, within these general parameters, can exercise discretion.

Formal Research and Audit Reports that are Incomplete (section 22(1)(h))

This provision covers the contents of formal research and audit reports that, in the opinion of the head of the public body, are incomplete. It provides protection against premature disclosure of information that could be misleading, inaccurate or incomplete.

Formal means that the research or audit reports have been compiled in accordance with procedures that ensure the validity of the research or audit process. The research or audit is carried out in accordance with a prescribed methodology to ensure the greatest degree of accuracy for the results.

Audit is defined as a financial or other formal and systematic examination or review of a program or activity, or a portion of a program or activity (**section 22(3)**).

Incomplete means that the report is in preliminary or draft format, is under review for accuracy or completeness, or is being reviewed to ensure that it meets the mandate of the research or audit proposal.

For this provision to apply, there should be some evidence that the research or audit report has not been finalized.

For example, if a consultant's research report had been accepted by a public body and payment made in full without any indication that the report had not fulfilled the mandate set out in the contract, the report would be complete. A report submitted by an auditor to officials of a public body for review and discussion prior to its formal presentation would be incomplete.

This exception applies only within a limited time frame. Once the report is accepted as complete, it cannot be protected under this exception. If the report is submitted but no further progress is made on it for a period of 3 years, it cannot be protected under this exception.

Progress implies some activity designed to finalize or complete the report, not simply a review of its contents with no subsequent action.

When the Exception Does Not Apply

Section 22(2) provides some specific cases where the exception in **section 22(1)** does not apply.

Information has been in Existence 15 Years or More (section 22(2)(a))

This provision means that any information contained within a record which has been in existence for **15** years or more cannot be withheld under the exception.

15 years means the period from a particular month and day to a corresponding month and day **15** years later. Other exceptions may still apply to the information.

A Statement of the Reasons for a Decision that is made in the Exercise of a Discretionary Power or an Adjudicative Function (section 22(2)(b))

This provision requires the release of formal judgments, including the reasons for reaching those judgments. The provision applies when the decision has already been made and is not merely contemplated.

Reasons mean the motive, cause or justification or facts leading to a decision.

Exercise of discretionary power is normally granted under statute to the administrative level of government. There is discretionary power when, given certain factual circumstances, the administrative authority is free to make a particular decision, given a range of options from which to choose.

Adjudicative function means a function conferred upon an administrative tribunal, board or other non-judicial body or individual that has the power to hear and rule on issues

involving the rights of people and organizations.

Reasons for decisions of this type cannot be withheld under **section 22(1)** despite the fact that the decisions may contain advice or recommendations prepared by or for a minister or a public body.

Results of Product or Environmental Testing (section 22(2)(c))

This provision excludes from the coverage of **section 22(1)** the results of product or environmental testing carried out by or for a public body. The testing has to be complete or have had no progress made on it for at least three years.

Examples would be information on a product such as air filters or the results of environmental testing at a land fill or testing of air quality in a building.

It does not apply to testing done:

- For a fee as a service to a person other than a public body; or
- For the purpose of developing methods of testing or testing products for possible purchase

Examples of test results covered under the exception would be the results of commercial product testing and soil testing. As well, the information may be withheld if the testing was done for the purpose of developing methods of testing. An example might be testing to develop a new drug evaluation methodology. There would have to be evidence in such cases that methodology development was the sole purpose of the testing.

The exception also covers test results where testing was done by a public body in order to determine whether or not to purchase a product.

Statistical Survey (section 22(2)(d))

This provision excludes from the coverage of **section 22(1)** statistical surveys.

Statistics is the science of collecting and analyzing numerical data and the systematic presentation of such facts.

Statistical surveys are general views or considerations of subjects using numerical data. Such reports may not be withheld under **section 22(1)**. Where statistical surveys appear with information that can be withheld under **section 22(1)**, the excepted information should be severed and the statistical survey disclosed.

An example of a statistical survey would be a study of growth rates in various forested areas of Prince Edward Island. Such a study would have to be released even though it may be part of a larger document dealing with reform of forestry law, regulation or policy.

The Result of Background Research of a Scientific or Technical Nature undertaken in Connection with the Formulation of a Policy Proposal (section 22(2)(e))

This provision excludes from the coverage of **section 22(1)** background research undertaken as the basis of formulating a policy proposal.

Background research encompasses a wide range of study, review and fieldwork aimed at analyzing and presenting an overview of issues.

For this provision to apply, the research has to be completed or have had no progress made on it for at least three years.

The research is to be scientific (conducted according to the principles of objective research) or technical (based on a particular technique or craft) and aimed at policy formulation. In order for information to be considered background research under this provision, it must be connected with the development of some specific policy. This would clearly be the case, if, for example, a policy proposal referred directly to the research on which the proposal was based.

Normally the research methodology, data and analysis cannot be withheld under **section 22(1)**. However, advice and recommendations contained in the same record as the background research or prepared separately by or for a public body or a minister could be withheld.

An Instruction or Guideline issued to the Officers or Employees of a Public Body (section 22(2)(f))

This provision excludes from the coverage of **section 22(1)** information used by officials in interpreting legislation, regulations or policy. It also excludes information used in exercising the discretion given to them under an Act of the Legislature or a by-law of a public body.

Generally, an official or employee in a position to provide interpretation or policy direction will have issued the instruction or guideline.

A Substantive Rule or Statement of Policy that has been Adopted by a Public Body for the Purpose of Interpreting an Act or Regulation or Administering a Program or Activity of the Public Body (section 22(2)(g))

This provision expands on the principles set out in **section 22(2)(f)**. It excludes from the coverage of **section 22(1)** the basic interpretations of the law, regulations and policy under which a public body operates its programs and activities.

4.12 ECONOMIC AND OTHER INTERESTS OF A PUBLIC BODY OR THE GOVERNMENT OF PRINCE EDWARD ISLAND

Section 23(1) of the Act provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to harm the economic interest of a public body or the Government of Prince Edward Island as a whole, or the ability of the government to manage the economy.

Section 23 is a discretionary exception. The information that can be excepted includes:

- Trade secrets of a public body or the Government of Prince Edward Island (**section 23(1)(a)**).
- Financial, commercial, scientific, technical or other information in which a public body or the Government of Prince Edward Island has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value (**section 23(1)(b)**).
- Information the disclosure of which could reasonably be expected to:
 - Result in financial loss to;
 - Prejudice the competitive position of; or
 - Interfere with contractual or other negotiations of the Government of Prince Edward Island or a public body (**section 23(1)(c)**); and
- Information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee or the public body of priority of publication (**section 23(1)(d)**).

This exception allows the public body discretion to protect information if its disclosure could harm either its own financial or economic interests or those of the Government of Prince Edward Island as an entity. It also protects information that would harm the ability of the Government of Prince Edward Island to manage the economy.

The exception refers to the *Government of Prince Edward Island* as a whole. This recognizes that public bodies, individually or collectively, may hold significant amounts of financial and economic information that is critical to the financial management of the public sector and the management of the provincial economy. **Section 23(1)** ensures that, where harm would result from disclosure, certain portions of this information may be withheld.

Harms Test

In order to use the exception, a public body must have objective grounds to believe that disclosure will likely result in the harm. The context in which a public body operates is taken into account in determining whether it is reasonable to expect that harm will result from the disclosure of the information.

Economic interests refer to both the broad interests of a public body and of the government as a whole, in managing the production, distribution and consumption of goods and services.

It also covers financial matters such as the management of assets and liabilities by a public body and the public body's ability to protect its own or the government's interests in financial transactions.

The *financial interests* of the Government of Prince Edward Island include the ability to collect taxes and generate revenues.

Harm to these interests includes damage or detriment to the economic policies or activities for which a single public body is responsible, as well as harm to policies and programs that affect the overall economy of the province. It also includes monetary loss or loss of assets with monetary value.

Examples of information the disclosure of which might qualify for harm to economic interests include:

- Information on a public body's investment strategies which affects its interests or future financial position.
- Information in budget preparation documents that could result in segments of the private sector taking actions affecting the ability of the government or a public body to meet economic goals.
- Information about licensing and inspection practices of a public body that could affect the amount of revenue collected.
- Information about a trade deal, a development plan or strategy or an economic negotiation that has not been completed.

Section 23(1) does not prevent the release of information that reveals a liability that might lead to a lawsuit against a public body for alleged wrongdoing.

In most cases, the public body whose economic interests are involved will be the public body with custody or control of the record(s) requested.

In some instances, however, a public body may hold information about another public body whose economic interests may be affected by disclosure. Consultation is essential between the two bodies in situations when use of **section 23(1)** is being considered.

Interests of the Government of Prince Edward Island

The exception may also be claimed for the *Government of Prince Edward Island* in the broad, corporate sense. The term *Government of Prince Edward Island* connotes a broader sense here than that of public body. The exception has a different and higher level coverage, since *government* is intended to convey the sovereign power of the state in carrying out its will and functions.

The phrase *ability to manage the economy* refers to the responsibility of the Government of Prince Edward Island to manage the province's economic activities by ensuring that an appropriate economic infrastructure is in place, and by facilitating and regulating the activities of the marketplace. This depends on a range of activities including fiscal and economic policies, taxation, and economic and business development initiatives.

Types of Information

The types of information listed in **section 23(1)** are illustrative only and may not cover all types of information that could reasonably be expected to cause harm to economic interests. At the same time, inclusion in one of the categories in **section 23(1)** is not by itself sufficient to allow a public body to refuse access. Application of this exception is subject to a harms test. A public body must have reasonable grounds to expect harm as a result of disclosure in order to apply the exception.

Trade Secret (section 23(1)(a))

Trade secret is defined in **section 1(n)** of the Act as meaning information, including a formula, pattern, compilation, program, device, product, method, technique or process:

- That is used, or may be used, in business or for any commercial purpose.
- That derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use.
- That is the subject of reasonable efforts to prevent it from becoming generally known.
- The disclosure of which would result in significant harm or undue financial loss or gain.

Information must meet *all* of these criteria to be considered a trade secret.

Information that is generally available through public sources (ex., published research reports) would not usually qualify as a trade secret under the Act.

A public body must own trade secrets or must be able to prove a claim of legal right in the information (ex., a licence agreement) in order to qualify for the exception. Normally, this

will mean that the trade-secret information has been created by employees of the public body as part of their jobs, or by a contractor as part of a contract with the public body.

For example, software developed by a public body or special testing equipment, which is not generally known, would have commercial value. Disclosure of the specifications could reasonably be expected to result in improper benefit and the information could probably qualify as a trade secret. On the other hand, details of a minor technical adjustment to equipment that has been inspired by an article in a trade journal would not qualify.

Section 23(1)(a) does not apply to trade secrets of a third party. Requirements relating to the protection of these are dealt with in **section 15(1)(a)**. See section 4.3 of this chapter.

Financial, Commercial, Scientific, Technical or other Information in which a Public Body or the Government of Prince Edward Island has a Proprietary Interest or a Right of Use and that has, or is reasonably likely to have, Monetary Value (section 23(1)(b))

The exception in this provision is subject to a three-part test. In order for the exception to apply, *all* of the following conditions must be met:

- The information must be financial, commercial, scientific, technical or other information.
- The public body or the Government of Prince Edward Island must have a proprietary interest or a right of use.
- The information must have, or be reasonably likely to have, monetary value.

Financial information refers to information relating to money and its use or distribution, or assets with monetary value, such as securities or stock options. Common examples are investment strategies and financial forecasts.

Commercial information refers to information concerning the sale, purchase or exchange of goods and services. Examples include marketing plans, pricing structures and customer records.

Technical information means information relating to a particular subject, craft or technique, such as systems design specifications.

Scientific information relates to experiments, principles and procedures derived by scientific method. An example would be a particular scientific testing methodology.

The second part of the test requires that the public body or the Government of Prince Edward Island have a *proprietary interest* in the information. This means that the public body or the government must be able to demonstrate rights to the information either through direct ownership or contractual rights or licensing agreements.

The third part of the test is whether the information has or is reasonably likely to have monetary value. *Monetary value* may be demonstrated by potential for financial return to the public body or government. Examples might be special computer software or a systems design which could be patented and or licensed and marketed for a profit.

Information the Disclosure of which could reasonably be expected to result in Financial Loss to, Prejudice the Competitive Position of, or Interfere with Contractual or other Negotiations of the Government of Prince Edward Island or a Public Body (section 23(1)(c))

This section provides similar protection for business enterprises in the public sector as is provided for private sector third parties under **section 14(1)(c)**). To claim the exception, a public body must have objective grounds for believing that one of the harms listed will result from disclosure.

In the case of *financial loss*, there must be reasonable grounds to believe that disclosure of information in the specific record would result in direct monetary loss or loss in terms of a monetary equivalent. This includes loss of revenue, loss of reputation or loss of good will in the marketplace. The loss cannot be speculative nor can it be loss expected as a result of a “ripple effect.”

Prejudice to competitive position means that a public body must have a reasonable expectation that disclosure of the information is capable of being used by an existing or potential competitor to reduce the public body’s or the government’s share of a market. However, the exception may be claimed whether or not there is currently a competitor in the marketplace.

Interfere with contractual or other negotiations means obstruct or make much more difficult the negotiation of a contract or other sort of agreement between the public body or the government and a third party. The expectation of interference with negotiations as a result of disclosure must be reasonable and the negotiations have to be specific, not simply potential negotiations of a general kind in the future.

Information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee or public body of priority of publication (**section 23(1)(d)**).

Public bodies employ a wide range of researchers, including professional scientists, technicians and social scientists. Their reputations are often dependent on the research they publish.

The fact that they have a professional reputation is of considerable value to public bodies that employ them. In addition, their research often has monetary and program value for the public bodies. For these reasons, the Act protects the priority of publication for all types of research.

Examples include scientific and technical research carried out at research institutes; historical research connected with the designation or preservation of historical or archeological resources; and epidemiological and other medical studies carried out in health care bodies. A public body would have to provide some proof that publication is expected to result from the research or that similar research in the past has resulted in publication.

When the Exception Does Not Apply

Section 23(2) provides that a public body must not refuse to disclose under **section 23(1)** the results of product or environmental testing carried out by or for a public body, unless the testing was done:

- For a fee as a service to a person, other than the public body (**section 23(2)(a)**); or
- For the purpose of developing methods of testing or testing products for possible purchase (**section 23(2)(b)**).

The intent of the provision is to ensure that a public body does not withhold information resulting from product or environmental testing carried out either by the employees of a public body or on its behalf by another organization. Examples include information on products such as air filters and environmental test results on water quality or air quality.

Information can be withheld when the public body performs the testing, for a fee, as a service to a private citizen or private corporate body. Common examples are commercial product testing and soil testing. The information may also be withheld if the testing was done for the purpose of developing methods of testing. An example might be testing to develop a new drug evaluation methodology. There would have to be evidence in such cases that methodology development was the sole purpose of the testing. The exception can also be used to withhold test results compiled to determine whether or not a public body would purchase a product. In all three circumstances, the harms test in **section 23(1)** still has to be met before the information can be withheld.

4.13 TESTING PROCEDURES

Section 24 of the Act provides that a public body may refuse to disclose information relating to:

- Testing or auditing procedures or techniques (**section 24(a)**);
- Details of specific tests to be given or audits to be conducted (**section 24(b)**); or
- Standardized tests including intelligence tests (**section 24(c)**).

The exception applies only if the disclosure could reasonably be expected to prejudice the use or results of particular tests or audits.

Section 24 is a discretionary exception.

This exception provides protection for the procedures and techniques involved in testing and auditing. It also protects details relating to specific tests to be given or audits to be conducted.

The terms *test* and *audit* are intended to be interpreted broadly to cover a wide variety of activities undertaken by public bodies or by the private sector on behalf of public bodies. Examples include environmental testing, staffing examinations, personnel audits, financial audits, and program audits.

Specific mention is made of standardized tests such as intelligence tests, psychological tests and aptitude tests. Information is protected where disclosure of a test or audit that is to be conducted, or is currently in process, would invalidate the results. This applies even if there is no intention to use the test or audit again in the future.

Information is also protected where there is an intention to use the procedure in the future, and disclosure would result in unreliable results being obtained and the test or audit having to be abandoned as a result. Test questions that are regularly used – for example, in making staffing decisions – may be protected from disclosure.

Information relating to a test or an audit that has been used in the past, but which is neither in process nor to be used in the future, is not protected by this exception. The exception applies to testing and auditing carried out both by public bodies and by consultants and contractors.

This section does not provide an exception for the results of tests or audits. This includes the results of standardized tests or intelligence tests. Public bodies should exercise care in disclosing such results by ensuring that a professional familiar with the tests is available to explain and interpret them to the applicant. This process may be specified in policy.

4.14 PRIVILEGED INFORMATION

Section **25** deals with legal privilege.

Section **25(1)** gives the head of the public body *discretion* to refuse to disclose information subject to legal privilege.

When dealing with information that may qualify for an exception under **section 25**, public bodies should always consult legal counsel.

Section 25(1) of the Act provides that a public body may refuse to disclose information:

- That is subject to *any type* of legal privilege, including solicitor–client privilege or

- parliamentary privilege (**section 25(1)(a)**);
- Prepared by or for the Minister of Justice and Public Safety and Attorney General, or an agent or lawyer of the Department of Justice and Public Safety, or an agent or lawyer of a public body, in relation to a matter involving the provision of legal services (**section 25(1)(b)**); or
- In correspondence between the Minister of Justice and Public Safety and Attorney General, or an agent or lawyer of the Department of Justice and Public Safety, or an agent or lawyer of a public body, and any other person in relation to a matter involving the provision of advice or other services by the Minister of Justice of Public Safety and Attorney General, the agent or lawyer (**section 25(1)(c)**).

Section 25(2) is a *mandatory* exception requiring the public body to *refuse to disclose* privileged information subject to legal privilege (as described in **section 25(1)(a)**) if it relates to a third party. When this occurs, the public body must refuse to disclose the information.

Section 25(3) provides that only the Speaker of the Legislative Assembly may rule on the question of what is and what is not parliamentary privilege. **Section 60(5)(a)** provides that the Commissioner cannot review the Speaker's ruling.

The intent of this section is to ensure that information privileged at law, as well as other similar information in the custody or under the control of a public body, is protected from disclosure in much the same way as an individual's information would be by their lawyer.

Section 25 is also intended to protect disclosure of privileged information in the custody or control of a public body that belongs to a third party, as well as information covered by parliamentary privilege.

The Act does not define *legal privilege*, so its definition is derived from the common law.

Subject to **section 25(2)**, when information falls within the scope of **section 25(1)**, a public body may decide to disclose the information if the law would otherwise permit disclosure. An example would be when the "owner" of the privilege consents to disclosure.

Legal Privilege - Nature of the Privilege

Section 25(1)(a) deals with any type of *legal privilege*, expressly including *solicitor-client privilege* and *parliamentary privilege*.

The Alberta Information and Privacy Commissioner has found that legal privilege exception in Alberta's Act incorporates the common law public interest privilege. **Section 25(1)(a)** of the Act mirrors Alberta's legal privilege exception.

Public interest privilege refers to a determination of whether information should or should not be disclosed. That determination requires that a decision-maker balance two competing

public interests: the public interest in maintaining the confidentiality of certain information and the public interest in disclosing the information.

There are two categories of privilege: “class privilege” and “case-by-case privilege.” Class privilege, which includes solicitor–client privilege, litigation privilege and police informer privilege, refers to a privilege where it is presumed that it is in the public interest to maintain the confidentiality of the information.

Case-by-case privilege requires a public body to weigh the policy reasons for maintaining confidentiality in each case and determine whether the public interest favours disclosure or non-disclosure.

Class Privileges

Solicitor–Client Privilege

The most recognizable class privilege is solicitor– client privilege. If a record is subject to solicitor-client privilege, the record is confidential and does not have to be disclosed.

Solicitor–client privilege is permanent and concerned with protecting communication between lawyers and clients in relation to the seeking or giving of legal advice. These communications are called solicitor and client communications. Without assurance of confidentiality, a client may not speak openly and candidly with legal counsel.

The presence of an agent does not destroy solicitor–client privilege, as long as the communication through the agent meets the tests discussed below.

Severing is not a concept recognized at common law; and as such, it is not applied to records subject to solicitor–client privilege. Therefore, the privilege is asserted over the entire record. It is notable that Alberta’s Information and Privacy Commissioner has stated that if solicitor– client privilege applies, it applies to the entire document. This has been followed in this jurisdiction. The Commissioner has no jurisdiction either to determine the factual component under the Rules of Court, or to require that the public body sever that document under Alberta’s legislation which in this regard mirrors section 25 of the Act.

Solicitor and client communications

In the case of solicitor and client communications, each record must meet the following criteria for the privilege to apply:

- It is a communication between solicitor and client.
- It entails the seeking or giving of legal advice.
- It is intended to be confidential by the parties.

The information must be contained in a communication between a solicitor and a client. A memorandum or note from one employee of a public body to another summarizing a conversation between that employee and the public body's lawyer does not meet this criterion. It may, however, still be properly excepted as part of a claim for privilege or meet the criterion of **section 25(1)(c)**, discussed below.

The term *legal advice* is defined to include a legal opinion about a legal issue, and a recommended course of action, based on legal considerations, regarding a matter with legal implications.

Both parties must intend the communication to be confidential, and must demonstrate that this confidentiality has been maintained. If confidentiality is not maintained, privilege is waived and privilege can no longer be asserted (see Waiver of Privilege below). A client's communication with their solicitor solely to convey or receive factual information may not be privileged under these criteria because the communication does not relate to the seeking or giving of legal advice. An example might be an invoice or the cover sheet of a facsimile transmission. On this premise, a solicitor's request to the client for factual information may also not be privileged.

The Information and Privacy Commissioner has the jurisdiction to determine whether a solicitor–client privilege claim has been properly made. However, in 2016, the Supreme Court of Canada concluded that the Alberta Information and Privacy Commissioner cannot compel production of records over which solicitor–client privilege has been claimed. The legal privilege provision in Alberta's legislation mirrors section 25 of the Act. As such, determination of whether a public body has satisfied all three criteria discussed above requires the Commissioner to consider the evidence provided by the public body and the context of the circumstances.

In addition, Alberta's Information and Privacy Commissioner has stated that Alberta's Commissioner has no jurisdiction to delve into any record to determine what part of a solicitor–client communication is factual and therefore not privileged under the rules relating to discovery of documents in court cases. In other words, only the courts can determine what parts of a document are factual and can be disclosed.

The following substantive rules may also be considered when a claim for solicitor–client privilege is made:

- The confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent.
- Unless the law provides otherwise, when and to the extent that the legitimate exercise of a right would interfere with another person's right to have their communications with their lawyer kept confidential, the resulting conflict should be resolved in favour of protecting the confidentiality.

- When the law gives someone the authority to do something which, in the circumstances of the case, might interfere with that confidentiality, the decision to do so and the choice of means of exercising that authority should be determined with a view to not interfering with it except to the extent absolutely necessary in order to achieve the ends sought by the enabling legislation.
- Legislation referred to above must be interpreted restrictively.

Records such as solicitor's briefing notes and working papers directly relating to the seeking or giving of legal advice may be excepted under this provision.

Where a communication between a solicitor and client constitutes a continuum of advice, such communication is privileged.

Litigation privilege

The criteria for litigation privilege are different from those that apply to solicitor–client communications. Further, litigation privilege is temporary and lapses when the litigation ends. To correctly apply this privilege, the public body must show that:

- There is a third party communication which may include:
 - Communications between the client (or the client's agents) and third parties for the purpose of obtaining information to be given to the client's solicitors to obtain legal advice;
 - Communications between the solicitor (or the solicitor's agents) and third parties to assist with the giving of legal advice; or
 - Communications which are created by the client, including reports, schedules, briefs, documentation, etc.
- The maker of the record or the person under whose authority the record was made intended the record to be confidential. The one exception is for the lawyer's "work product" or "lawyer's brief" for which it is the lawyer's intention that is relevant when the lawyer assembles material for the brief for litigation.
- The *dominant purpose* for which the records were prepared was to submit them to a legal advisor for advice and use in litigation, whether existing or contemplated. The *dominant purpose* test consists of three requirements:
 - The records must have been *produced* with existing or contemplated litigation in mind;
 - The records must have been produced for the *dominant purpose* of existing or contemplated litigation; and
 - If litigation is contemplated, the prospect of litigation must be reasonable;
- The confidentiality must not be waived.

The guiding principle for litigation privilege is that all papers and materials created or obtained especially for the lawyer's brief for litigation, whether existing or contemplated, are privileged.

This means that such papers and materials are confidential and do not have to be disclosed.

The privilege applies to papers and materials:

- Created or obtained by the client for the lawyer's use in existing or contemplated litigation; or
- Created by a third party or obtained from a third party on behalf of the client for the lawyer's use in existing or contemplated litigation.

When determining *dominant purpose*, the intent of the maker of the record or the person under whose authority the record was made is to be considered.

Furthermore, the maker of the record or the person under whose authority the record was made *must* have intended the record to be confidential, with the possible exception of the "work product" or "lawyer's brief" rule.

Waiver of Privilege

The right to solicitor–client privilege belongs to the client and not the lawyer, and may be waived by the client. This allows a public body to disclose records that fall within the parameters of **section 25(1)**.

A client may also waive litigation privilege; and as previously noted, litigation privilege lapses when litigation ends.

Waiver can occur in one of two ways:

- An intention to waive the privilege; or
- More commonly, a waiver by implication.

An example of where an intention to waive occurs is when the client specifically waives the privilege. This may occur through a decision to disclose information to a third party, whether in response to an access request under the FOIPP Act or not, or through widespread dissemination of the information.

This does not occur when records are copied to lawyers or employees within the public body. Nor does it occur when records have been copied to legal firms which provided solicitors to represent the public body, or to the Minister to whom the public body reports. Privilege is not waived when an individual is obliged to comply with a public body's requirements under penalty of enforcement proceedings for non-compliance.

Waiver by implication is less clear. Waiver in these circumstances may occur where fairness and consistency require it, such as in a court case where the client directly makes an issue out of the legal advice given. There can also be a *deemed waiver* where part of a record containing solicitor–client privilege is released or where privilege is not claimed for the entire communication on a page.

If a public body cannot provide evidence that confidentiality has been maintained, the public body can be found to have waived solicitor–client privilege.

There can be a *limited waiver* of privilege, which does not extend to a waiver for other purposes. For example, a third party might voluntarily provide public documents to a public body, but that does not constitute a waiver of privilege to other parties. There can also be a privilege in aid of anticipated litigation in which several persons have a common interest such that, in providing records to each other, the parties with common interests do not waive privilege as against other parties or the world at large. In considering whether a limited waiver can stand, it will be important to check to whom records may have been formally copied.

Police Informer Privilege

Another class privilege is an informer, historically known as *police informer privilege*.

This privilege prevents not only disclosure of the name of the informer, but also any information that might implicitly reveal identity, even if it is the smallest detail.

The privilege afforded to police informers has been granted in order to give protection to citizens who assist in law enforcement. These individuals may very well be vulnerable to reprisals from those against whom they inform.

The policy reason behind the privilege is to protect this source of information since, without the privilege, the information would likely not be provided. The end result would be that the policing agencies would be impaired in their efforts to detect and prevent crime.

Although the privilege belongs to the Crown, the privilege also belongs to the informer. The only way the privilege can be waived is with the informer’s consent, or, in the case of an anonymous informer, by the Crown.

The privilege is subject to only one exception: “innocence at stake.” To raise this exception, there must be a basis on the evidence for concluding that disclosure of the informer’s identity is necessary to demonstrate the innocence of someone in a criminal proceeding.

An analogy may be made to police informer privilege in other situations. It will be necessary to show that the public interest in protecting communications to government agencies by informers outweighs the public interest in requiring that the information be

produced in proceedings under the relevant legislation such as the *FOIPP Act*.

This occurs when the public body requires this information in order to administer legislation dealing with public health and safety.

This does not apply to employees of a public body whose job it is to provide information about suspected fraud or other infringements of legislation that they administer.

Parliamentary Privilege

Parliamentary privilege is a unique class privilege that provides the necessary immunity to allow members of the Legislative Assembly to do their legislative work.

As discussed above, section 25(3) provides that only the Speaker of the Legislative Assembly may determine whether information is subject to parliamentary privilege.

If the Speaker makes a ruling that records are subject to parliamentary privilege, the Information and Privacy Commissioner has no jurisdiction to review a decision of a public body to refuse to provide access to those records **section 60(5)(a)** of the Act.

In addition, the Speaker remains free to make such a determination even after the Speaker has decided that the records are not subject to exceptions contained in the Act.

When a public body believes that all or parts of the records that are the subject of a request may be subject to parliamentary privilege, it must provide notice to the Speaker of the Legislative Assembly. The notice must include a description of the contents of the record(s) and a request that the Speaker determine whether or not parliamentary privilege applies to some or all of the information. The decision of the Speaker *must* be followed.

Legislated Privilege

A class legal privilege also can be established by an act or by a regulation.

New Class of Privilege

It has been said that to find a new class of privilege for private records, compelling policy reasons must exist similar to those underlying the privilege for solicitor–client communications, and the relationship must be inextricably linked with the justice system.

Identification of a new class of privilege on a principled basis is not precluded. But it has also been said that the extension of the doctrine of privilege consequently obstructs the truth-finding process and, accordingly, the law has been reluctant to proliferate areas of privilege unless an external social policy is demonstrated to be of such unequivocal importance that it demands protection.

Case-By-Case Privilege

For a case-by-case privilege to exist, the decision-maker must determine whether the public interest favours disclosure or non-disclosure in a particular case.

Records may be either *private records* or *Crown records*. *Crown records*, that is, provincial government records, include records containing information relating to activities, operations or decisions at the highest level of the provincial government such as Cabinet decisions.

Private Records

Private records are records in the hands of a third party where there is a reasonable expectation of privacy, such as medical or therapeutic records, private diaries, and social worker activity logs, etc. For case-by-case privilege to be recognized, the following four criteria must be met:

- The communications must originate in a confidence that they will not be disclosed.
- This element of confidentiality must be essential to the full and satisfactory maintenance of the relationship between the parties.
- The relationship must be one which in the opinion of the community ought to be diligently fostered.
- The injury that would result to the relation by the disclosure of the communications must be greater than the benefit gained for the correct disposal of the litigation.

The criterion that the injury from disclosure must be greater than the benefit from disclosure for the privilege to apply requires an assessment of the interests served by protecting communications from disclosure. This includes privacy interests and the inequalities that may be perpetuated by the absence of protection. The balancing exercise under this criterion is essentially one of common sense and good judgment. It must also be kept in mind that a request for access and an inquiry under the Act are not litigation.

The balance to be struck is that the injury to the relationship from the disclosure of the information must be greater than an applicant's right of access to the information under the Act. An informer's privacy interests are struck at a different level in a proceeding under the Act than in civil proceedings and more easily outweigh an applicant's right of access under the Act.

Crown Records: Public Interest Immunity or Crown Privilege

Historically, the privilege for Crown records has been called *Crown privilege*. It is more properly called *public interest immunity* because there must be a balancing of two competing public interests:

- The public interest in non-disclosure to maintain government secrecy.

- The public interest in disclosure for the proper administration of justice.

For a case-by-case privilege to attach to Crown records, the Crown must put forward a claim based on the following criteria for public immunity:

- The nature of the policy concerned.
- The particular contents of the records.
- The level of the decision-making process.
- The time when a record or information is to be revealed.
- The importance of producing the records in the administration of justice, with particular consideration to:
 - The importance of the case.
 - The need or desirability of producing the records to ensure that the case can be adequately and fairly represented.
 - The ability to ensure that only the particular facts relating to the case are revealed.
- Any allegation of improper conduct by the executive branch towards a citizen.

Privilege Relationship with Legal Agent

Section 25(1)(b) and (c) deal with circumstances where a legal privilege may not exist.

Section 25(1)(b) is about information prepared by or for the Minister of Justice and Public Safety and Attorney General or by or for an agent or lawyer of the Department of Justice and Public Safety or an agent or lawyer of a public body. That information must be prepared *in relation to* a matter involving the provision of legal services.

The term *legal services* is given its ordinary dictionary meaning, and includes any law-related service performed by a person licensed to practice law, including the Attorney General.

This provision is broader than solicitor–client privilege. It appears to protect information that would not be protected by solicitor–client privilege.

Section 25(1)(c) covers correspondence between the Minister of Justice and Public Safety and Attorney General or an agent or lawyer of the Department of Justice and Public Safety or an agent or lawyer of a public body and any other person in relation to a matter involving the provision of advice or other services.

This provision covers only correspondence, and that correspondence must relate to a matter involving the provision of advice or other services.

A memorandum or note from one employee of a public body to another summarizing a conversation between that employee and the public body's lawyer may or may not meet this criterion.

Legal Privilege of Other Persons

As noted above, section 25(2) requires public bodies to protect information described in **section 25(1)** when it relates to a person other than a public body.

At times, privileged legal records of an individual or other third party come under the custody or control of a public body. In these circumstances, the public body has an obligation to protect these legal records.

The distinction between this provision and **section 25(1)(a)** is that **section 25(2)** is *mandatory*. The public body must not disclose the information if the criteria in **section 25(1)(a)** and **25(2)** are met.

This provision speaks of *information* that relates to a person other than the public body and not a *record* or *document*. It is meant to encompass not only another person's records or documents to which the privilege under **section 25(1)(a)** might apply, but also *information*, in any form, to which a privilege applies.

Records in which a public body has discussed or otherwise reproduced a third party's privileged information may also be covered by this provision.

Information under **section 25(1)(a)** also "relates to" persons other than a public body if they supplied the information and the information can identify them.

Even if a record of this nature was disclosed before the coming into force of the Act, because **section 25(2)** is a *mandatory* exception, a public body is obliged to apply it if a record is within the scope of the exception.

Relationship with Section 15, Section 18 and Section 20

Section 15(4)(b) and **section 18(1)(d)** have not incorporated into the Act a public interest privilege for private records in the custody or control of the Crown. The Act also does not preclude **section 25(1)(a)** from incorporating the common law public interest privilege for private records.

Section 20 of the Act does not appear to incorporate the common law as to public interest privilege or public interest immunity for certain specific Crown records, namely Cabinet confidences.

4.15 DISCLOSURE HARMFUL TO ARCHAEOLOGICAL SITES, HERITAGE PLACES, RARE, ENDANGERED OR VULNERABLE LIFE

Section 26 provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to result in damage to or interfere with the conservation of:

- Any archaeological site as defined in the *Archaeological Sites Protection Act* (**section 26(a)**);
- Any heritage place as defined in the *Heritage Places Protection Act* (**section 26(b)**); or
- Any rare, endangered, threatened or vulnerable form of life (**section 26(c)**).

Section 26 is a discretionary exception. It enables a public body to protect information about archaeological sites, heritage places and rare or endangered forms of life which, if disclosed, could result in damage to or interference with conservation measures. If a public body has records that might fall under this exception, it may consult with the ministry responsible for the *Archaeological Sites Protection Act* and the *Heritage Places Protection Act* in making a decision on disclosure.

In using this exception there must be objective grounds to believe that disclosure is likely to result in damage to or interference with conservation measures.

Definitions

The *Archaeological Sites Protection Act* defines *archaeological site* as land of prehistorical or historical significance that has been designated as an archaeological site.

The *Heritage Places Protection Act* defines *heritage place* as a place in the province which includes or is comprised of any work of nature or of man that is primarily of value for its palaeontological, archaeological, prehistoric, historic, cultural, natural, scientific or aesthetic interest.

Damage refers to destruction, disturbance, alteration, deterioration or reduction in the value of an historic resource.

In **section 26(c)**, the following general definitions apply:

A *rare form of life* is any species of flora or fauna that is in a special category because it does not occur in great abundance in nature, either because it is not prolific or its population or range has been adversely affected by modern civilization.

An *endangered form of life* is any species of flora or fauna that is threatened with extinction throughout all or a significant portion of its natural range.

A threatened form of life is any species of flora or fauna that is likely to become endangered in Canada or Prince Edward Island if the factors affecting its vulnerability are not reversed.

A vulnerable form of life is any species of flora or fauna that is of concern because it is naturally scarce or likely to become threatened as a result of disclosure of specific information about it.

4.16 INFORMATION THAT IS OR WILL BE PUBLISHED

Section 27(1) provides that a public body may refuse to disclose information:

- That is available for purchase by the public (**section 27(1)(a)**);
- That is to be published or released to the public within 60 days after the applicant's request is received (**section 27(1)(b)**); or
- Readily otherwise available to the public (**section 27(1)(c)**).

Section 27 is a discretionary exception.

The provision enables a public body to refuse to disclose information that is currently available for purchase by the public. This allows the public body to follow its normal procedures for selling information, if its policy has been to do so, or to make a decision to publish particular information. The Act is not intended to replace existing procedures for access to information (**section 3(a)**). It also provides for a public body to decide whether or not to withhold information that will be published or released within 60 days of the applicant's request.

Available for Purchase

Available for purchase by the public means that a publication is generally available for purchase from the public body or a government or private bookstore. It must be available to the general public, not only to a limited group such as realtors or an interest group. In such instances, the public body must tell the applicant where the publication may be purchased. Examples include maps, research reports, catalogues, and telephone directories.

About to be Published

There will be situations when a request is made for information that is about to be published. There may be a desire to claim the exception in **section 27(1)(b)** for a number of reasons. The publication may be required by the Legislative Assembly and the Minister or head cannot or will not release the information first through another channel. The public body may wish to control the date when the information is made public. As well, it may

also be more convenient and economical to await the publication date.

The exception covers only the manuscript being published and not surrounding data or research and background material. These records will have to be dealt with separately, if requested, or if the applicant cannot be convinced that the request is satisfied by receipt of the publication.

Section 27(1)(b) may only be claimed if there are no legal impediments to publishing, such as **Part 2** of the FOIPP Act.

The public body should have a copy of the information to which it is denying access readily available in order that it can be published or released in the requisite time frame. In order to claim **section 27(1)(b)**, the public body should have an active publication or release plan that establishes a date when the information will be available to the public.

The 60 days for publication or release is from the date of receipt of the applicant's request and not from the date when a response is made to the request.

It is important that a public body ensure that the requested records are either published or released to the public within the 60-day time frame established by the provision.

Released to the public means made available to the public at large either through active dissemination channels or through provision of the information at specific locations (e.g., public libraries).

Section 27(1)(c), this provision enables a public body to refuse to disclose information that is readily available to the public.

Readily available to the public means currently accessible to the general public. For example, may be available through a website, in a public library, in a public directory or in a manual available to the public for copying.

Notification of Applicant

Section 27(2) requires the head of the public body to notify an applicant of the publication or release of information that the head has refused to disclose under **section 27(1)(b)**.

Such notification should provide:

- The date of publication or release.
- The specific location where the applicant can have access.
- How access will be given.
- The purchase price, if this is relevant.
- Any other information that the public body is required to give the applicant under **section 10(1)** of the Act.

If there is no charge for the publication, the public body could simply provide a copy to the applicant on publication.

Failure to Publish

Section 27(3) states that if the information is not published or released within 60 days after the applicant's request is received, the head of the public body must reconsider the request. This must be done as if it were new request received on the last day of that period, and access to the information must not be refused under **section 27(1)(b)**.

This means that on the 60th day the head of the public body is required to consider the applicant's request as a new request with 30 days to respond, dating from that day. The public body cannot employ the "publishing or release" exception in any consideration of the new request.

CHAPTER 5

Third Party Intervention and Notice

5.1 OVERVIEW

Many public bodies hold large quantities of information about individuals, companies, non-profit groups and other third parties. The Act recognizes that disclosure of this information might result in harm to these third parties (see Chapter 4.3 and 4.4). The Act provides for notification of third parties when access to records containing such third party information is requested.

A *third party* is defined in **section 1(m)** as a person, a group of persons, or an organization other than an applicant or a public body. It includes individuals, sole proprietorships, partnerships, corporations, unincorporated associations and organizations, non-profit groups, trade unions, syndicates, trusts, and their legal representatives.

5.2 WHEN IS THIRD PARTY NOTIFICATION REQUIRED?

Section 28 of the FOIPP Act applies when a request has been received for a record containing information that may be withheld under **section 14**, disclosure harmful to the business interests of a third party, or **section 15**, disclosure harmful to personal privacy.

Section 28(1) requires that a public body provide written notice to a third party when it is considering giving access to a record that may contain information described in **sections 14** and **15**. It is a *mandatory* provision.

Section 28(1) also does not apply when a public body invokes **section 27(1)** to respond to the request. **Section 27(1)** allows an exception to disclosure for information that is available through purchase, or will be published or released to the public within sixty days of receiving the request. As well, **section 28(1)** does not apply when a public body seeks advice from a third party about disclosure under another section of the Act. An example of this would be consultation with a federal government department under **section 19(2)**.

Section 28(1.1)

A notice under **section 28** is not normally given under the following circumstances. Notice is not normally given when a public body is disclosing a record containing information in **section 15(2)(j)**.

Disclosure of this information is not considered to be an unreasonable invasion of personal privacy. **Section 28(2)** states that the requirement to give notice established in **section 28(1)** does not apply to a record containing information to which **section 15(2)(j)** applies.

It is important that public bodies take steps to give individuals an opportunity to request non-disclosure under **section 15(3)** when personal information subject to **section 15(2)(j)** is collected, because third party notice will not be given in these cases.

Notice is not normally given when a public body is relying on the Act's exception to disclosure for information that is or will be available to the public (**section 27(1)**). **Section 28(1.1)** states that the requirement to give notice under **section 28(1)** does not apply to information that a public body may refuse to disclose in accordance with **section 27**.

Section 28(2) provides that a public body may give written notice to a third party even though it intends to refuse access to records under **section 14** or **15**.

This provision allows a public body to give a third party the opportunity to consent to disclosure of information that the public body intends to refuse to disclose. It also allows a third party that objects to disclosure of the information concerned to provide additional information in support of non-disclosure. This may be useful to a public body in defending its refusal to provide access before the Information and Privacy Commissioner.

The provision for notice to a third party when a public body does not intend to disclose third party information also permits a public body to provide notice to clients who may be third parties in an access request. The clients can be made aware that a request for information concerning them has been made before an applicant requests a review by the Information and Privacy Commissioner.

A public body can also provide a less formal notification, such as a telephone call. This might take place when a public body is very certain of its grounds for refusal of access and does not need representations from a third party to support this decision. Such an informal notice has no standing under the Act and is merely a courtesy to the third party.

Public bodies must ensure that they do not reveal the identity of the applicant in any communication, whether formal or informal, with a third party.

There is no obligation to undertake third party notice when a public body is intending to refuse access to information under **section 14** or **15**.

5.3 HOW IS A THIRD PARTY NOTIFICATION PROCESS CARRIED OUT?

Section 28(1) requires that third party notice be given "where practicable and as soon as practicable." This means that third party notice must be given unless, after reasonable attempts to locate and notify the third party, it is impossible to do so. Such notice must be given as soon as possible in order to respond to the request within a reasonable time frame.

Public bodies are expected to use only their own records and publicly available resources in trying to locate an address for a third party.

Notices must be in writing. **Section 28(1)** covers notice to the third party and **section 28(4)** states that, when a notice is given to a third party, a notice must also be provided to the applicant.

Where possible, these notices should be given at the same time. If more than one person or organization is affected by the disclosure of information in a record, a notice has to be given to each affected third party.

Section 70 requires that any notice or document to be given to a person under the *Act* be given:

- By sending it to that person by prepaid mail to the last known address of that person;
- By personal service;
- By substituted service if so authorized by the Commissioner; or
- By means of electronic or other telecommunication messaging.

Public bodies should choose a delivery method that ensures that the notice arrives quickly and conveniently for the third party, but which is also efficient and cost-effective for the public body. Prompt delivery will allow the third party as much time as possible to respond.

Under normal circumstances, the public body sends notices to the third party and the applicant by mail (regular mail or priority post). Where possible and practical, a notice may be sent by fax, with originals following by mail. In exceptional circumstances, it may be necessary to send a notice by courier or registered mail.

If sending the notice by fax or other electronic means, care should be taken to prevent unauthorized disclosure of third party information. It may be necessary to telephone the third party before sending the notice to identify the individual best suited to deal with it or to advise of the electronic transmission.

Personal service means a method of delivery whereby it can be shown that the person to be served actually received the document.

Substituted service means the placing of public notices in a trade journal or in other specialized or general media. This is normally intended for situations where a very large number of third party notices are required or where a third party cannot be located and the nature of the information would lend itself to this type of public notice.

When notice by substituted service is contemplated, a public body should enter into a full consultation with the Office of the Commissioner about why it believes such notice is appropriate in the particular case. Substituted service can only be used with the permission of the Commissioner.

5.4 CONTENT OF THIRD PARTY NOTICE

Section 28(3) states that a third party notice must:

- Contain a statement that a request has been made for access to a record that may contain information the disclosure of which would affect the interests or invade the privacy of a third party.
- Either include a copy of the record, or the part of it containing the information in question, or include a full description of the contents of the record involved.
- Contain a statement that, within 20 days after the notice is given, the third party may, in writing, either consent to the disclosure or make representations explaining why the information should not be disclosed.

Efforts should be made to ensure that the third party understands the significance of the notice, and also that only those matters pertinent to the applicability of **section 14** or **15** are relevant to the response. It must be clear that the public body cannot consider comments or statements on other exceptions when it makes its decision regarding the applicability of these exceptions.

The third party response must be in writing. A verbal response is not satisfactory for the purposes of **section 28**. The identity of the applicant must not be included in the notice sent to the third party, unless the applicant has consented to this disclosure. The notice must include the name, job title and telephone number of the person within the public body that the third party may contact for more information. Good communication with the third party is a key to ensuring a smooth notification process and promoting better understanding of the third party's representations when determining the applicability of the exception.

5.5 NOTICE TO APPLICANT

Section 28(4) provides that, when notice is given to a third party, the public body must also provide a notice to the applicant.

The notice must state that:

- The requested record may contain information the disclosure of which would affect the business interests or invade the personal privacy of a third party
- The third party is being given an opportunity to make representations respecting disclosure.
- Decision whether or not to give access to the requested record(s) will be made within 30 days after the date of notice to the third party.
- The identity of the third party is not included in the notice sent to the applicant.

5.6 RESPONSE FROM THIRD PARTY

In deciding whether or not to give access to all or a portion of the requested record(s), the public body must consider any third party responses received in reply to notices given under **section 28(1)** which are pertinent to **section 14** or **15**, as applicable.

Section 29(1) provides that a public body must decide whether or not to give access within 30 days of giving notice. However, a decision cannot be made until the third party responds, or on the 21st day after notice is sent, whichever comes first.

Consent

If the third party consents to disclosure of the information, the public body releases the information unless another exception in the Act applies to it. The public body should be satisfied that the person giving consent to disclose information on behalf of a business or other organization is an officer, employee or corporate officer authorized to provide such consent.

Non-Disclosure

If a third party makes representations as to why the information should not be disclosed, the public body considers the representations in reaching a decision on access. If there is any doubt that the third party has understood the significance of the notice or the criteria that apply in decisions regarding access, the public body should contact the third party by telephone to discuss the matter.

Non-Response

If a third party does not respond to the notice within 20 days of the sending of the notice, the public body must make a decision based on the information available.

Failure to respond does not imply the third party's consent to the disclosure of the information. The public body must not draw any inference from the lack of a response.

Public bodies should contact the third party by telephone, fax or electronic mail to discuss why a response has not been made. The opportunity for contact extends up to the point of disclosure of the information. It may be helpful in the event of a review by the Commissioner for the public body to be able to provide documentation of its efforts to contact a third party.

5.7 NOTICE OF DECISION

Section 29(2) provides that once a public body has made a decision on access, it must give notice of this decision to both the applicant and the third party. This notice will vary according to circumstances.

When Access is Permitted

Applicant: The public body informs the applicant of the decision and the reason for it, and provides notice that access will be provided in 20 days if the third party does not ask for a review by the Information and Privacy Commissioner.

Third Party: The public body informs the third party of the decision and the reason for it, and provides notice that the third party can request a review of the decision by the Commissioner within 20 days after the date of the notice.

The public body cannot disclose the information until after the 20 days allowed for the third party to request a review.

When Disclosure is Denied

Applicant: The public body informs the applicant of the decision and the reason for it, and provides notice that the applicant may, within 60 days, request a review of the decision by the Information and Privacy Commissioner.

Third Party: The public body informs the third party of the decision and the reason for it, and advises that the applicant may, within 60 days, request a review of the decision by the Information and Privacy Commissioner.

5.8 TIME LIMITS

Section 9(1) states that a public body must make reasonable efforts to respond to a request within 30 calendar days of its receipt. The third party notification process allows the head of a public body to extend that time limit. Public bodies should not use this extension of time to unnecessarily delay responding to the applicant. Time extensions under **section 12** should be carefully considered (see Chapter 5.9 of this publication).

The major time limits are:

- Third party notice is given as soon as possible, and, for the most part, within 30 days from the date the public body received the request.
- Third parties have 20 days to respond to the notice.
- No decision can be made until this response is received, or 21 days after notice is given, whichever comes first.
- The public body must make a decision within 30 days after the notice is given (i.e., it has at least 10 days to consider the responses and make the decision).
- After notice of a decision is given, a third party has 20 days to ask for a review.
- After notice of a decision is given, the applicant has 60 days to ask for a review.

It is not necessary to seek permission from the Commissioner for time extensions required to comply with the requirements of **section 29** with respect to the time allowed for the third party notification process and the time allowed for a third party to request a review.

Notice to Third Parties

This notice should be sent as soon as possible after the receipt of a request, and normally within 30 days of receipt of the request, unless the time limit has been extended for a reason other than third party consultation.

The 20-day time period allowed for a third party to respond to a notice begins on the day after the public body sends the notice, not the date the third party receives it. The date on which the notice is sent is the date marked on it indicating posting or electronic transmission (e.g., the postmark for regular mail, and the transmission date for e-mail or facsimile). For example, if a public body sends a third party notice by regular mail and the envelope is postmarked March 1, the third party has until March 21 to respond.

Response from Third Party

The third party has 20 days after the notice is given to respond, either by consenting to the release of the information or by making representations as to why the information should not be released. If no response has been received by the 21st day after the notice was given, the public body decides, on the basis of the available information, whether or not to give access to the record.

Decision by Public Body

The public body is required to decide whether or not to give access to all or part of the record within 30 days after the third party notice is given.

Section 29(1) states that the public body may not make this decision until after the third party has had an opportunity to respond to the notice. Since the third party has up to 20 days to respond, the public body cannot make a decision on access until the earlier of:

- 21 days after the notice was given under **section 28(1)**.
- The day a response is received from the third party.

Notice of Decision

By the 30th day after notice was given to the third party, the public body must give written notice of its decision regarding access to the record to both the applicant and the third party, but it does *not* give immediate access to the record.

Review of Decision

When the decision is to release all or part of the record(s), the third party has 20 days after the notice is given to ask the Information and Privacy Commissioner to review the decision. This 20-day period is calculated from the day after the public body gives the notice, not from the date the third party receives it.

It is important to note that the third party has only 20 days in which to request a review, not 60 days as allowed under **section 61(2)** in other instances.

This shorter period reflects the fact that the third party has already had time in which to prepare arguments on why information should not be disclosed.

Where the decision is to refuse all or part of the record(s), the applicant has 60 days to request a review in accordance with **section 60(1)**.

Access to Record

If the decision of the public body is to give access to a record or part of a record despite the representations of the third party:

- The public body must wait for a 20-day period after the notice of decision is given before the applicant is given access. This 20-day period allows the third party time to ask the Commissioner to review the decision.
- If the third party does not request a review within the 20-day period, the applicant is given access to the records that were the subject of third party representations on the 21st day.
- A public body may contact the Office of the Information and Privacy Commissioner to determine whether a request for review has been submitted.
- If the third party does request a review by the Commissioner, then the time limit for responding to the request is extended under **section 12(1)(d)**. The applicant is not given access to any record or part of a record that is the subject of the review until the review is completed. If the review affects only some of the records proposed for disclosure, the public body releases the remainder of the records to the applicant.
- The outcome of the review determines whether or not access is given to any record that is the subject of review.

The public body should provide the applicant with access to those records not affected by third party representations or subject to any other exception without waiting for the outcome of any consultation or review.

5.9 TIME LIMIT EXTENSION

If the third party notice is given early in the request management process and the third party responds promptly and has no objections to disclosure, the public body may be able to respond within the original time limit of 30 days from the receipt of the request, as allowed under **section 9**.

In most cases, more time will be needed for third party consultation. Generally, the period of 30 days after the date of notice (as allowed under **section 29(1)**) plus the period of 20 days for the third party to request a review (as allowed under **section 29(3)**) provides all the time necessary for the completion of the third party consultation process and no further extension is needed.

In some cases, however, additional time may be needed to complete third party consultations and make the decision on access. A public body may extend the time limit beyond:

- The original 30-day limit allowed under **section 9**; or
- The longer period allowed under **section 12(1)(a)** or **(b)** to the extent required to enable the public body to comply with the requirements of **section 29** regarding third party consultation and right of review. Any longer extension must be requested in writing and approved by the Information and Privacy Commissioner.

Additional time may be needed in the following circumstances:

- The public body must consider a large number of third party representations; or
- The public body needs to consult further with third parties to clarify representations.

If possible, the public body makes the decision on whether or not an extension is needed when it gives notice to the third party and the applicant under **section 28**. If the public body cannot make an informed estimate of the time required for third party consultations at the time notice is given under **section 28**, it may be necessary to delay the decision on extension until the responses have been received.

Situations may also arise where a public body has already claimed an extension (e.g., to process a large number of records) and then discovers third party information that requires a notice. The time for the third party notification process will carry the time beyond the 60-day limit that could be claimed through an extension by the public body under **section 12(1)**.

In such circumstances, the third party must have up to 20 days in which to make representations.

The public body would then extend the time limit to allow an additional 20 days for these representations. A public body would also extend the time for response by 20 days after making a decision to disclose information in order to allow a third party to ask the Commissioner to review that decision.

If the third party requests a review by the Commissioner, the public body should consult with the Commissioner about the length of time needed for the review to take place.

The applicant has the right to make a complaint to the Information and Privacy Commissioner about any time limit extension.

CHAPTER 6

Disclosure in the Public Interest

6.1 OVERVIEW

Section 30(1) of the FOIPP Act establishes a public interest provision that obliges the head of a public body to disclose information without delay when:

- The information is about a risk of significant harm to the environment or to the health or safety of the public, a group of people, a person or the applicant; or
- The disclosure is, for any other reason, clearly in the public interest.

This provision applies whether an access request has been made or not.

Disclosure may be to the public, to an affected group of people, to any person or to the applicant.

This is a *mandatory* provision. Any information that meets the criteria set out in the provision must be disclosed even if there has not been a formal request under the *Act*.

The provision further requires that action be taken *without delay*. The assumption is that any circumstances that would warrant consideration of **section 30** would be urgent, and that no delay should occur where disclosure is demanded by events that have an impact on public safety or where disclosure is in the public interest.

The circumstances may have developed over a period, but disclosure without delay may be required when the situation has reached a critical point. The actual assessment of what constitutes *without delay* must be made on a case-by-case basis. Some factors that should be considered in the assessment are:

- The level of harm anticipated.
- The degree of risk that the harm will occur.
- The imminence of the harm, that is, whether there is a clear and present danger of significant harm.
- Measures that could be taken to avoid the harm and the amount of time required for these measures, and whether release of information would likely reduce the risk of the harm.
- The importance of consulting with other public bodies whose interests may be affected by the disclosure.
- The right of a third party to make representations.
- The right of the public to make informed choices about the risks to which they are exposed.

6.2 DISCLOSURE

Section 30 of the Act refers to *information* not *records*. Where a request for disclosure in the public interest is made by an applicant as part of a FOIPP request, the decision of the public body will, most likely, be focussed on particular records.

Where no FOIPP request is made but the public body is considering disclosure in the public interest to the general public, an affected group of people or a person other than an applicant, the emphasis will almost always be on *information* as opposed to *records*. Disclosure might be of the facts surrounding an event or issue as opposed to the documents recording those facts.

This distinction means that the public body might release only basic or summary information and not the whole record on an event, subject or issue that affects the public interest.

For example, a public body might release the location, nature and extent of the contamination of a building or site but not necessarily all the scientific, exposure, emergency response and property records that relate to the event.

Section 30 anticipates disclosure in four different ways:

- To the public generally;
- To an affected group of people;
- To any person; or
- To an applicant making a request.

Disclosure to the Public

Where the public interest dictates disclosure to the general public, the public body must ensure that the information is released in a manner designed to reach the public at large. Examples include the use of radio, television, newspapers, and electronic networks.

An example would be disclosure about an armed or dangerous criminal who is suspected to be in a particular area of Prince Edward Island. In this case, disclosure would be to the general public in that particular area.

Disclosure to an Affected Group

Where the information relates to circumstances that affect only a specific group of people, rather than the public at large, the head must ensure that effective ways are used to reach the affected group. If the information is of a sensitive nature, it is important that steps are taken to ensure that only the affected group is informed.

For example, if a safety hazard, such as an unstable trench, were discovered at a workplace, only those people on site who could come into contact with the hazard until it was fixed would need to be warned.

Disclosure to Any Other Person, including an Applicant

Where information relates to any other person, including an applicant, the public body must employ notification measures that provide the information to the person concerned and no one else, unless the public interest dictates wider disclosure of the information.

An example would be disclosure of the fact that an individual has been released on parole and continues to threaten the safety of their spouse.

In all cases, only the minimum amount of personal information necessary to alert the public concerned about the risk should be disclosed.

6.3 PUBLIC INTEREST

Section 30 provides for disclosure in the public interest where the information is:

- About a risk of significant harm to the environment or to the health or safety of the public; or
- For any other reason, clearly in the public interest.

Risk of Significant Harm to the Environment or to Health and Safety

Risk is generally taken to mean the chance, possibility or certainty of danger, loss, injury or other adverse consequences.

The determination that there is a risk of harm to the environment or to public health or safety is usually made by professionals working for the public body or contracted by the public body to assess situations where there is a possible risk of harm. Determining the nature and extent of the risk is part of the management process.

Inclusion of the term *significant* in this provision means that the head of a public body must be convinced that the harm risked is considerably greater than in normal circumstances.

Harm to the environment refers to the damage to or degradation of any component of the earth, including air, land, and water; any layers of the atmosphere; and any organic and inorganic matter. It also includes damage to or degradation of the interacting natural systems that include components of these things, through either natural calamity or illegal or improper use. An example might be information about toxic emissions from an industrial plant.

Harm to health means damage to the well-being of the body or mind of an individual, or the health of the general public. An example of a risk of significant harm to health might be the contamination of a water supply.

Harm to safety means a condition where an individual or the general community does not feel safe and free from danger or risks. A risk of significant harm to safety might be created by a natural gas leak or a bomb threat that threatens an explosion in a populated area.

In Alberta, this section of the Act, together with an Alberta Justice Protocol for the application of the provision, has been used to release personal information on the whereabouts of violent offenders released from correctional facilities who are still considered by law enforcement and parole officials as a serious risk to a community.

Public, Affected Group of People, Any Person or Applicant

Section 30(1)(a) applies to information that reveals a risk of significant harm to the general public, a specific group of people, or an individual, including an applicant.

Other Public Interest

Section 30(1)(b) is a general clause intended to cover any other situation where the head of a public body may decide that disclosure of information is in the public interest. Such disclosure must be *clearly in the public interest*. This means that the case for release in the public interest is, in the opinion of the head, beyond reasonable doubt. The information involved must be a matter of compelling public interest and not just of interest or of curiosity to the public, a group of people, a person or the applicant.

6.4 DETERMINATION OF PUBLIC INTEREST

The determination of *public interest* will have to be made on a case-by-case basis and requires a balancing of the public interest in release of the information on the one hand and the public and private interests in protecting the information from disclosure on the other.

Examples where disclosure in the public interest might be considered are situations where:

- A public body has been alerted about a contagious disease or about an individual who is the carrier of a contagious or dangerous disease.
- A violent or dangerous offender has been released into the community.
- An individual seeking employment in child care on the basis of a false resume is found to have a history of child molestation that is recorded in a register of employment references for child-care workers.
- Information has come to light about corruption or serious misuse of public funds.

These are only illustrative examples where the public interest *might* be involved and situations will have to be judged on a case-by-case basis.

The burden of proof lies with the public body to show that **section 30** ought *not* to be applied since it has a positive obligation to apply it where necessary.

Public bodies may wish to consider in advance the conditions or criteria that might be typical of their programs where **section 30** would be considered. It is recommended that a senior official in the public body retain the authority for decisions on **section 30**.

6.5 SCOPE

Section 30(2) provides that this section of the *Act* overrides all other sections of the *Act*.

This means that, if there is a risk of significant harm to the environment or to public health or safety, or disclosure is clearly in the public interest (**section 30(1)**), a public body must disclose information, including essential personal information, despite:

- The exception to disclosure of information harmful to personal privacy in **section 15** of the *Act*.
- The privacy protection provisions relating to disclosure of personal information in **section 37** of the *Act*.

The public interest disclosure provision represents a very significant exception to the rules for privacy protection, and any disclosure under **section 30** of the *Act* should be carefully considered and justified.

6.6 NOTIFICATION

Section 30(3) provides that, before disclosing information under **section 30(1)**, the public body must, if practicable:

- Notify any third party to whom the information relates.
- Give the third party an opportunity to make representation.
- Notify the Commissioner.

Normally, notice must be given to affected third parties and the Information and Privacy Commissioner *before* the information is released under **section 30(1)**.

However, this obligation to notify third parties and the Commissioner must be balanced against the obligation to disclose the information without delay. Notification is to take place only *where practicable*, and the head of the public body must ensure that there is no delay adversely affecting the public interest.

The factors governing release *without delay* outlined in section 6.1 of this chapter also apply here.

Such notice should take a similar form to the notice required by **section 28(1)** of the Act. Given the urgency of the situation, it should be delivered by fax or courier and accompanied by a telephone call advising the third party of the importance of making any representations by similarly expeditious means. Depending on the urgency, the third party may be asked to respond immediately or may be given a period of time.

The third party notice should be sent to any person, group of persons or organization, other than the person who made the request or a public body, that is a subject of the information or the record(s).

A similar notice, or a copy of the one sent to the affected person together with a covering note, must be sent to the Information and Privacy Commissioner to inform that office that a disclosure in the public interest is being made.

Section 30(4) requires that, where notification is not practicable under **section 30(3)**, the head of the public body must give written notice of disclosure:

- To the third party or parties
- To the Commissioner

Section 13 of the FOIPP Regulations requires the notice under **section 30(4)** to be in the form set out in **Schedule 3** of the FOIPP Regulations.

A copy of the letter and a covering note can serve as notice to the Information and Privacy Commissioner.

6.7 REVIEW

If there is a complaint about the failure of a public body to release information in the public interest, the Information and Privacy Commissioner can review the head's decision:

- *If a FOIPP request has been made*, under the powers provided in **section 60(1)** of the Act, which enables an applicant to request a *review* of the decision and prescribes a process for this to occur.
- *If no FOIPP request has been made*, under the general powers of the Commissioner in **section 50(1)** of the Act, which permits the Commissioner to monitor how the Act is administered to ensure that its purposes are achieved.

The powers of the Information and Privacy Commissioner are discussed in more detail in Chapter 8 of this publication.

6.8 DISCLOSURE TO THE COMMISSIONER

Section 69(1) of the Act provides that an employee of a public body may disclose to the

Commissioner any information which that employee is required, whether under oath or by agreement, to keep confidential, if the employee, acting in good faith, believes that the information:

- Ought to be disclosed by the head of the public body under the public interest provisions of **section 30**; or
- Is being collected, used or disclosed in violation of the privacy provisions contained in **Part 2** of the Act.

The Commissioner will seek proof that the employee is acting in *good faith*. This means that the employee has an honesty of intention or honestly believes that they are following a lawful path. If the Commissioner is satisfied that the complaint is in good faith, there must be an investigation of the disclosure (**section 69(2)**).

The Commissioner is forbidden to divulge the identity of the employee except with that individual's consent (**section 69(3)**).

Disclosure can occur through written communication with the Commissioner or through a meeting between the employee and the Commissioner or one of the Commissioner's staff delegated to undertake the case.

If an employee acted in good faith, they are protected from prosecution under any Act for:

- Copying a record or disclosing it to the Commissioner; or
- For disclosing information to the Commissioner (**section 69(4)**).

An employee acting in bad faith would not be protected from prosecution.

Bad faith means acting with mischievous, harmful or false intent.

A public body or any person acting on behalf of a public body is prevented from taking any adverse employment action against an employee acting in good faith who:

- Has disclosed information to the Commissioner under this section; or
- Has exercised or *may exercise* a right under this section (**section 69(5)**).

Any person who violates the principles and rights set out in **section 69(5)** is guilty of an offence and liable to a fine of not more than \$10,000 (**section 69(6)**).

The intent of the section is to give balanced and adequate protection to employees. This is to encourage employees to come forward when they honestly believe that the public body for which they work is:

- Either ignoring an important public interest in failing to release particular information; or
- Is failing to meet the obligations to protect personal privacy imposed by the provisions of **Part 2** of the FOIPP Act.

CHAPTER 7

Protection of Privacy

7.1 OVERVIEW

Part 2 of the FOIPP Act establishes conditions and obligations that public bodies must meet in protecting the privacy of individuals whose personal information is in their custody or under their control. The provisions are based on the international privacy standard issued by the Organization for Economic Cooperation and Development (OECD) and commonly known as the OECD Privacy Guidelines. Canada became a signatory to this standard in 1984.

These OECD Guidelines were used as the basis for the development by the Canadian Standards Association of the *Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96).

The *FOIPP Act* is generally consistent with the principles set out in the *Model Code*. While the *Model Code* does not apply to public bodies, it has been adopted voluntarily by a number of private-sector organizations and forms the basis of the federal *Personal Information Protection and Electronic Documents Act*.

Sections 31 to 40 of the Act establish controls over the collection, use and disclosure of personal information and requirements for protecting, correcting, retaining, and ensuring the accuracy of the information.

Personal information is recorded information about an identifiable individual. The extent and nature of personal information is defined in **section 1(I)** of the Act.

The provisions relate to *all* personal information in the custody or under the control of public bodies, *except* for personal information that is outside the scope of the legislation (see Chapter 1.7 of this publication on exclusions from the Act and the effect of paramountcy).

Public bodies that hold personal information to which the Act does not apply should bear in mind that it is good business practice:

- To inform individuals about the purpose of collecting their personal information.
- To take steps to ensure the accuracy of personal information.
- To protect personal information from unauthorized access, use or disclosure.

Public bodies collect and retain information for a variety of purposes that are essential to their effective and efficient operation.

The FOIPP legislation requires public bodies to balance operational efficiencies against the interests of individuals in their own information and privacy. This balance is achieved by good information management practices, including controls over the collection of information by public bodies, the disclosure of information for a variety of public purposes, and electronic information system design. These privacy protection measures are often referred to as a *code of fair information practices*.

The Act provides that public bodies must:

- Give individuals access to their own personal information and the opportunity to request correction of errors or omissions in it.
- Collect personal information only for purposes authorized under an enactment, for law enforcement, or when needed to operate programs or for other activities.
- Collect personal information directly from the individual concerned unless the individual authorizes collection from another person, or the Act authorizes indirect collection.
- Notify individuals about the authority for and purpose of collecting their personal information unless such notification will lead to the collection of inaccurate information.
- Use and disclose personal information only for the purpose for which it was collected, for a consistent purpose, or for a purpose set out in the Act.
- Make reasonable efforts to ensure that the personal information they collect for decision-making purposes is accurate and complete.
- Retain personal information used for decision-making purposes for at least one year after it has been used so that individuals may exercise their rights of access and correction.
- Make reasonable security arrangements to protect personal information in their custody or under their control.

Part 2 of the Act, Protection of Privacy, may be best implemented if the FOIPP Analyst ensures that close cooperation occurs with program directors or managers responsible for personal information holdings, the Senior Records Officer and the head of Information Technology, in organizations where these centers of responsibility exist.

It is important to understand **Part 2** of the legislation in relation to **Part 1**, Freedom of Information. **Part 1** deals with the access process under the Act when an applicant submits a FOIPP request. **Part 2** addresses the manner in which personal information must be handled by public bodies at all times.

Part 1 establishes a right for individuals to access information about themselves (**section 6(1)**), and this is complemented in **Part 2** by the right to request correction of that personal information (**section 34**).

Part 1 also incorporates, in **section 15**, a balancing test to determine whether or not release of personal information would be an unreasonable invasion of personal privacy. This test comes into play whenever an applicant other than the individual the information is about, or that individual's personal representative, makes a request for a record containing personal information.

For more information on the exception for disclosure of information harmful to personal privacy, see Chapter 4.4 of this publication.

This provision is complemented by **section 37**, which applies, in the absence of an access request, to regulate the disclosure of personal information to parties other than the individual the information is about. **Section 37** governs disclosure of personal information both in response to external requests and in the internal business activities of public bodies.

Part 2 applies equally to public bodies and to persons, groups and organizations acting on behalf of a public body under contract. These contracts must stipulate clearly the privacy requirements of the Act imposed on the public body and ensure the contractor assumes them.

7.2 PURPOSES OF COLLECTION

Section 31 of the Act provides that no personal information may be collected by or for a public body unless:

- The collection of personal information is expressly authorized by or under an enactment of Prince Edward Island or Canada;
- The personal information is collected for the purposes of law enforcement; or
- The personal information relates directly to and is necessary for an operating program or activity of the public body.

Collection occurs when a public body gathers, acquires, receives or obtains personal information. It includes activities where individuals respond through interviews, questionnaires, surveys, polling, or by completing forms in order to provide information to public bodies. There is no restriction on how the information is collected. The means of collection may be writing, audio or video taping, electronic data entry or other such means.

Section 31 of the Act stipulates that collection can take place *by or for* a public body. A public body is bound by the requirements of the Act whether it conducts its own collection activities or authorizes an outside agent to carry out the collection. This authorization may be either under contract or through an agreement or arrangement with another public body or private organization.

When collection of personal information is carried out by one public body on behalf of another public body, this must be done under a written agreement. The agreement should state the reasons for collecting information in an indirect manner, the specific authority for the collection, and the purposes for which the personal information will be used or disclosed. Any use or disclosure of the personal information must be authorized under the Act.

When an outside organization or contractor is collecting personal information on behalf of a public body, the public body must have in place a written agreement or contract. This must stipulate how the organization or contractor will meet the requirements of the Act regarding the collection, use, disclosure, security, retention and disposition of the personal information being collected.

Section 31(a) provides that collection may be expressly authorized by an enactment of Prince Edward Island or Canada. This means that collection may find its authority in either provincial or federal statute or provincial or federal regulations.

In some Acts, there is detailed provision for the collection of certain specific types of personal information. In these cases, the statute both authorizes collection and identifies the personal information that can be collected. More commonly, the Act will authorize a program or activity, and a regulation under the Act will provide detailed authority for collection and sometimes the format in which the information is to be collected.

If an enactment authorizes a program or activity, but there is no specific authorization for the collection of information for the purposes of the program or activity, a public body cannot rely on the enactment as authority for collection of the information.

Section 31(b) permits the collection of personal information for the purposes of law enforcement. *Law enforcement* is defined in **section 1(e)** the Act and further explained in Chapter 4.7 of this publication.

Section 31(b) recognizes that law enforcement agencies must engage in wide-ranging information collection that would not always be allowed under the more restrictive terms of **section 31(c)**.

It would be difficult for a law enforcement agency to show, at the moment of collection, how each piece of personal information collected for investigative or enforcement purposes relates directly to or is necessary for the activity under way. Certain investigative methods, such as taking witness statements, might be seriously compromised by limiting the collection of personal information.

Section 31(c) permits the collection of personal information when that information:

- Relates directly to.
- Is necessary for, an operating program or activity.

Most often, legislation will only give authority for a particular program or activity, without authorizing the collection of specific personal information. Public bodies must then determine the exact elements of personal information which they need to administer a particular program and design collection instruments to obtain this information *and no more*. Collection authority then derives from **section 31(c)** of the Act.

Relates directly to means that the personal information must have a direct bearing on the program or activity.

Necessary for means that the public body must have a demonstrable need for the information.

The word *and* is restrictive. The collection must meet both parts of the two-part test in order for the public body to use **section 31(c)** as authority to collect personal information.

For example, if a program provides a particular benefit or service, information will be needed to ensure that an individual is eligible or qualified for that benefit or service. Personal information not related to the particular benefit or service is not required and should not be collected, even though it may be potentially useful to another program in the same public body.

An *operating program* is a series of functions designed to carry out all or part of a public body's operations. An *activity* is an individual action designed to assist in carrying out an operating program.

An important part of administering **section 31** involves public bodies undertaking a regular review of their current collection of personal information to ensure that it meets one of the three purposes discussed above.

Such a review should:

- Seek to clarify authorizations for collection of personal information.
- Eliminate any collection of personal information that does not meet the criteria set out in **section 31** and amend collection instruments, contracts and agreements, and policies and procedures that require the collection of this personal information.
- Ensure that information that is needed for subsets of clients is collected *only* for those clients.
- Implement administrative controls that continue to ensure that all new or modified collections of personal information meet the criteria set out in **section 31** and ensure that the minimum personal information necessary to meet program needs is collected.
- Implement administrative controls to ensure that any irrelevant personal information that is sent to a public body is placed in a separate file so that it is not improperly used, and that it is destroyed at an appropriate time after completion of the process for which the information was inadvertently collected.

This review should be carried out by the program areas having custody or exercising control over personal information, with the advice and cooperation of the FOIPP Analyst.

Administrative controls can be established in privacy standards, which should be included in the policy governing the overall collection activities of a public body. New collection activities and instruments should be reviewed by the FOIPP Analyst.

7.3 MANNER OF COLLECTION

Section 32(1) states that, subject to some limited exceptions, a public body must collect personal information directly from the individual the information is about. This establishes direct collection as the primary method for obtaining personal information.

This is an important principle of fair information practices. It helps to ensure that an individual is aware of the type of personal information being used to make a decision concerning them.

A public body must not, unless it is authorized to do so in the exceptions to this provision, seek the information from another source, even though it may have the capability of doing so.

Exceptions to Direct Collection

The Act provides for a number of circumstances where personal information about an identifiable individual may be sought from sources other than the individual the information is about.

Another Method of Collection Authorized by the Individual Concerned or Another Act or Regulation (section 32(1)(a))

This provision allows another person or organization to provide personal information about an individual under one of the specified conditions. If the provision applies, information may be provided orally, through written correspondence, electronic information exchange or file transfer.

When an individual authorizes the collection of their personal information from another source, this authorization should be in writing. This may take the form of a signed authorization on an application form or a letter giving authorization.

If authorization is less formal, as in a case where an individual provides authorization orally over the telephone, the public body should document the conversation and, whenever possible, send a letter to the individual concerned setting out what they have consented to.

When asked to consent to indirect collection of personal information under **section 32(1)(a)(i)**, the person should be informed of:

- The nature of the personal information to be collected.
- The purpose of the indirect collection.
- The reasons for making the collection indirectly.
- The consequences of refusing to authorize the indirect collection.

Information that may be Disclosed Under Division 2 of Part 2 of the Act (Use and Disclosure of Personal Information) (section 32(1)(b))

This provision permits a public body to collect personal information from a second public body, rather than from the individual the personal information is about, where the second body is authorized to disclose such information under **sections 36 to 39** of the Act.

Section 32(1)(b) provides the connection between use and disclosure on the one hand, and indirect collection on the other.

Where public bodies rely upon this provision to collect personal information indirectly, the public body that has the information must be satisfied that the disclosure is authorized. The public body receiving the information must ensure that it has authorization to collect it under **section 31**.

This provision recognizes the legitimate sharing of personal information between public bodies in limited and controlled circumstances, and the fact that more than one public body may need exactly the same personal information. It reduces the burden on the public to provide information to public bodies, as well as the cost of collecting personal information to operate programs and activities.

Information Collected for the Purpose of Law Enforcement (section 32(1)(c))

This provision allows law enforcement bodies to collect personal information indirectly when it is needed in investigations. It is obvious that a law enforcement body will not always collect information about a suspect only from the suspect themselves.

Much personal information about a person who is under investigation is collected from other sources. Reasons for this include the fact that investigators may not wish to alert the individual concerned that an investigation is taking place, the individual would not provide accurate information, or the individual might alter or destroy evidence. See Chapter 4.7 of this publication for information on the definition of law enforcement.

Information Collected for the Purpose of Collecting a Fine or Debt Owed to the Government of Prince Edward Island or a Public Body (section 32(1)(d))

This provision allows either a representative of the provincial government, as a whole, or of any individual public body to contact any person or organization that may be able to help in the collection of money owed to the public body or the government. This may include finding the home or work location or telephone number of the individual who owes money.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

A *fine* is a monetary punishment imposed on a person who has committed an offence.

When public bodies face the problem of not being able to locate those owing money, or when they believe they would not obtain accurate information needed to collect the debt from direct sources, they are permitted to collect personal information from other sources.

Information Concerning the History, Release or Supervision of an Individual Under the Control or Supervision of a Correctional Authority (section 32(1)(e))

This provision permits correctional and parole authorities to seek out information from a variety of sources about individuals under their control or supervision. The individuals may be in a correctional institution or may be supervised in the community.

History here means information about the person's background, including employment record, medical condition and behaviour.

Release includes both permanent and temporary release from a correctional institution.

Supervision includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of an individual held in a correctional institution.

Information Collected for Use in the Provision of Legal Services to the Government of Prince Edward Island or a Public Body (section 32(1)(f))

This provision recognizes that lawyers representing the provincial government or a public body may have to collect personal information to perform their jobs. The information may be required for day-to-day provision of legal services, or in the preparation for a proceeding before a court or tribunal.

Very often the nature of such activities precludes direct collection of the personal information because inaccurate information may be given. It may also be desirable that legal inquiries be made in confidence, or it may be that the individual concerned may not be able to provide the required information. In these circumstances the public body's legal representatives, or others providing legal services, can collect information indirectly, or ask an employee to do so on their behalf.

Information Necessary to Determine Eligibility to Participate in a Program or Receive a Benefit, Product or Service from the Government of Prince Edward Island or a Public Body and Collected in the Course of Processing an Application by the Individual the Information is About (section 32(1)(g)(I))

This provision recognizes that many programs operated by public bodies have eligibility criteria that must be met in order for an individual to participate in them or receive a benefit or service. This may require the public body to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met.

This collection of information can only take place in the course of processing an application from the individual, or from their representative. It is good business practice to inform the individual about whom information is being collected that information from a variety of sources will be collected to document a particular application. A statement of consent, signed by the individual, can be included on the application form.

The program, benefit, product, or service may be one offered on behalf of the provincial government or may be specific to a particular public body.

Information Necessary to Verify Eligibility to Participate in a Program or Receive a Benefit, Product or Service from the Government of Prince Edward Island or a Public Body and Collected for that Purpose (section 32(1)(g)(ii))

This provision is intended to allow for cases where an individual has already qualified for a program, benefit, product, or service and a public body needs to check to determine whether the eligibility remains valid.

In this case, personal information may be collected from a variety of sources other than the individual the information is about, and the individual may not be informed that verification is taking place.

For example, random checks of sources of information on the income and assets of individuals on social assistance or in low-income housing may be made to determine whether or not an individual remains eligible for the program. Such a check may involve an interview with the individual but may also involve collection of personal information about an individual from other sources.

Another example would be verification of a student's continued enrolment in a program in order that the student may continue to receive student financial assistance or a grant. As with the previous provision, it is good business practice to inform the individual about whom the information may be collected that verification of continuing eligibility may occur without notice. This is especially the case if the individual may incur any penalty for receiving a benefit for which they have become ineligible.

Information Collected for the Purpose of Informing the Public Trustee or a Person Exercising Public Guardianship Functions about Clients or Potential Clients (section 32(1)(h))

The *Public Trustee* is the trustee for dependent adults who are unable to administer their own financial affairs because of a mental disability. The Trustee also administers the estates of persons who die intestate if the deceased persons have no adult beneficiaries residing in the province.

In addition, the Trustee acts as guardian by protecting the assets and financial interests of missing persons and children under 18 years of age.

The *person exercising public guardianship functions* is charged with the responsibility of ensuring that appropriate surrogate decision-making mechanisms, supports and safeguards are available to assist adults who are unable to make personal decisions independently. This provision permits personal information to be collected indirectly from relatives, friends and others about anyone who is or may become a ward of the Public Trustee or the person exercising public guardianship functions. This may include information about the individual's mental or physical health, financial information, employment or educational history, and opinions about the individual.

Information Collected for the Purpose of Enforcing a Maintenance Order Under the *Maintenance Enforcement Act* (section 32(1)(i))

This provision permits the Director of Maintenance Enforcement to collect personal information about a separated or divorced spouse under certain circumstances. Where information cannot be gathered directly from an individual who has defaulted on maintenance support payments – because that person either cannot be located or is resisting the court order for maintenance – information may be collected from public bodies and other sources. This allows the Director to locate the defaulting spouse and enforce a maintenance order set down by a court.

Information Collected for the Purpose of Managing or Administering Personnel of the Government of Prince Edward Island or a Public Body (section 32(1)(j))

This provision allows government departments and public bodies subject to the *Civil Service Act* to collect personal information about an employee or potential employee from sources within the Government of Prince Edward Island. The provision recognizes the provincial government as the employer for all provincial departments.

Section 32(1)(j) also allows public bodies to collect information about employees or potential employees from third parties. Any collection under this provision must have, as its purpose, the management or administration of the personnel of the public body collecting the information.

Management or administration of personnel includes all aspects of the management of human resources of a public body. It includes staffing, job classification, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training, separation, and layoff. It does not, however, include management of consultant, professional or other personal services contracts.

Employees should be informed in a general way as to how personnel information about them is collected and from what sources they can expect this information to be derived. They should also be aware of the purposes for which various types of information are used and of their rights under the Act.

Examples of such collection include the collection of references for potential employees, determination of qualifications and performance for secondment and training opportunities, and the provision of pay and benefit services by one public body for other public bodies.

This provision refers to official personnel activities and does not sanction the collection of personnel-related information by individual officials for purposes other than official duties relating to the management and administration of personnel within a public body.

Information Collected for the Purpose of Assisting in Researching or Validating the Claims, Disputes or Grievances of Aboriginal People (section 32(1)(k))

This provision permits a public body to collect personal information indirectly in order to research the background and expedite the settlement of wider rights of aboriginal people.

Validating means confirming rights that have been contended by the parties to a claim, dispute or grievance.

The term *claims, disputes and grievances* is interpreted broadly to include all manner of controversies, debates and differences of opinion regarding issues in contention and is not restricted to differences over land claims.

Aboriginal people means individuals whose racial origins are indigenous to Canada.

Information Collected in a Health or Safety Emergency (section 32(1)(l))

This provision allows emergency services personnel, as well as other employees of a public body, to collect information needed to deal with an emergency situation.

This can happen when:

- The individual is not able to provide the information directly; or
- Direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person.

Examples of such emergency situations include cases where an injured person is not able to respond to questions about medication; accident or fire situations when a delay in collecting information about a person's actions could result in death or severe complications; cases where an unconscious person is suspected of having a communicable disease; and cases where treatment information is required from a physician or pharmacist.

Only information needed to deal with the emergency should be collected indirectly.

Information about an Individual who is Designated as a Person to be Contacted in an Emergency or Other Specified Circumstances (section 32(1)(m))

This provision allows for the collection of the name, relationship, address and telephone number(s) of an emergency contact. The individual may be a family member or a friend. Normally this information would be collected from the individual who is required to provide an emergency contact.

Such information is often provided when, for example, a public body hires a new employee.

Information Collected for the Purpose of Determining Suitability for an honour or Award (section 32(1)(n))

This provision allows a public body to seek references and other personal information about someone being considered for an honour or award. This includes honorary degrees, scholarships, prizes, and bursaries.

The nature of some awards is such that the potential recipients do not have to apply for the award and may not be aware that they are being considered. Scholarships and bursaries are often awarded on the basis of academic achievement and recommendations by faculty members; honorary degrees are usually awarded in recognition of a person's contribution to a community or sector of society; and prizes may be awarded on the basis of athletic or scholastic achievements.

Any information collected should be directly related to the honour or award being bestowed. Once the individual has been informed about the honour or award, they should be asked to consent to any future disclosure of personal information collected in connection with the honour or award.

Information Collected from Published or Other Public Sources for Fund-Raising (section 32(1)(o))

This provision allows for limited collection of publicly available personal information without the consent or knowledge of an individual. The information collected can be used only for fund-raising purposes.

Public bodies should keep such information segregated in their records and allow access by only those employees engaged in fund-raising and fund development activities.

Published sources are those that are normally available in print form or in some other generally accessible form such as audio tapes or video tapes.

Examples include newspaper reports, clipping files, corporate reports of public companies, and articles in periodicals. Most of this information would be readily available in a public or specialized library.

Other public sources include information that is generally available to the public, either free or for a fee, but is not necessarily published in a commercial format or as a matter of course.

Examples include information available on the Internet, information in reports of charitable organizations, announcements of honours or awards granted by or through a public body in Prince Edward Island, and copies of speeches or speaking notes when the speeches are given at a public event.

Not included under this provision is information of a more private character, such as information based on personal acquaintance, friendship or observation that may be provided by members of a governing board or employees, information that could only be gathered through surveillance or from private sources, patient or next-of-kin information, or names of parents of students.

Notification

Section 32(2) sets out rules that a public body must follow when it is required to collect personal information *directly* from an individual. A public body must inform the individual of:

- The purpose for which the information is collected.
- The specific legal authority for the collection.
- The title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

The requirement to provide notification applies only in those situations where information is collected *directly* from an individual.

The requirement to notify recognizes the individual's right to know and understand the purpose of the collection of personal information and how the information will be used. It also allows the person to make an informed decision as to whether or not to give personal information when there is no statutory requirement to do so.

Notification may be given in many ways. It may be:

- Printed on a collection form;
- Contained on a separate sheet or in a brochure accompanying a form;
- Published in an information brochure about a program;
- Displayed on a notice hung on the wall or placed on a service counter; or
- Given verbally.

A notification, consisting of the three elements set out in **section 32(2)**, should appear on or accompany all forms used to collect personal information directly from individuals. The same form of notice is required for computer-generated forms, regardless of whether an employee of the public body enters the information about the individual or the individual does the entry.

Notice should be given to individuals at the beginning of an interview when an individual is being asked to provide their own personal information. If the interview is being recorded, it is good practice to record the notice at the beginning of the tape. When individuals are applying for and participating in extensive and complementary programs, it may be more convenient and effective to place a generic notice in a publication about the programs, or explain orally. However, it is important that the individual is given an opportunity to make an informed decision as to whether or not to give the information and understand any consequences that may result from not doing so, including any limitations on services that the public body may provide in the absence of the information. This applies when information is collected over the telephone as well as in other cases.

When a notification is given verbally, either in person or over the telephone, care should be taken to ensure that the individual is informed of the privacy requirements in the Act. An explanatory document can be provided either at the counter or later by mail. It is also good practice to provide written confirmation of telephone collection of personal information.

It is good practice for a public body to provide an applicant with a copy of the notice and to retain a copy on file.

The *purpose* of a collection means the reason for which the information is needed and the use(s) that the public body will make of the personal information.

The *legal authority* for collection may be an enactment of Prince Edward Island or Canada that expressly authorizes collection of the personal information, or **section 31(c)** of the FOIPP Act, which authorizes collection of personal information that is directly related to and necessary for an operating program of a public body.

If a public body relies on **section 31(c)** of the FOIPP Act, it is important to provide the authority for the program. This is to increase people's awareness of the actual authority by which public bodies collect personal information. The program itself may be authorized by a provincial or federal Act or a regulation under an Act, or a by-law or legal resolution of a public body establishing a program that falls within its mandate under an Act.

Identifying someone to answer the individual's questions about the collection is intended to provide the individual with a knowledgeable source of information. The person cited should be familiar with the program, and be able to explain why the personal information is being collected and how it will be used, retained, and disclosed to other organizations.

Public bodies should undertake regular review of their collection instruments to determine which ones require the inclusion of collection notices.

Collection notices should be included on all forms used to collect personal information directly. This should be done in conjunction with the review discussed in **section 7.2** of this chapter.

Exception to Notification

Section 32(3) provides that the requirement of **section 32(1) and (2)** may be set aside if, in the opinion of the head of the public body, compliance with these provisions could reasonably be expected to result in the collection of inaccurate information.

This provision recognizes that in certain limited circumstances, such as the conduct of some surveys seeking opinions and in some psychological testing, there may be difficulty in getting accurate information if individuals are informed in advance of the reasons for the collection.

An example of a situation where a public body might not reasonably expect to obtain accurate information directly from the individual concerned would be the collection of information about participants in a literacy program who cannot read, write or understand English.

Inaccurate information is wrong, incomplete or misleading information, or information which does not reflect the truth. In the case of some surveys, notifying individuals of the purpose of the survey would lead to responses that would distort the results.

This provision is intended to be used in limited circumstances and public bodies should maintain documentation of when the provision has been used and the reasons for using it.

7.4 ACCURACY AND RETENTION

Section 33 of the Act provides that, if a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must:

- Make every reasonable effort to ensure that the information is accurate and complete.
- Retain the personal information for at least one year after use and shorter terms may be agreed to in writing by the individual, public body and the body that approves the retention and disposition for the public body.

A decision that directly affects the individual is one that has an immediate impact on the person's life. The meaning of the term is interpreted broadly and includes decision-making processes that are internal to a public body and those which involve a more direct relationship with the public.

Examples of decisions that directly affect an individual include a determination as to whether or not someone is entitled to income assistance, a decision on hiring an individual, or a determination regarding eligibility for health services.

This requirement does not extend to situations where no decision, adverse or otherwise, will be or has been made about an individual. Examples include raw survey data where personal information is collected but the results are rendered anonymous, telephone messages, and unsolicited resumes that are never considered in relation to a position.

Accuracy

Section 33(a) requires the public body to make every reasonable effort to ensure that personal information is accurate and complete.

A public body makes *every reasonable effort* when it is thorough and comprehensive in identifying practical means to assure that personal information in its custody or under its control is accurate and complete.

Generally, if a public body collects personal information directly, it is likely to meet the requirement of making every reasonable effort. This is especially so if the individual has signed a statement indicating that the information is complete and accurate.

Compliance with this provision involves careful verification of any personal information crucial to an application, transaction or action at the time the information is provided. A public body should also have systematic processes for updating personal information when it is used on a regular or continuous basis. This can be done using information provided by the individual or cross-referencing other related files providing basic identifying data.

Other checks of accuracy might consist in having periodic audits of files with accuracy and completeness as one of the criteria tested; ensuring limited access to information for the purpose of making corrections; and establishing cross-referencing and verification checks within the software of automated systems that identify anomalies in data.

The accuracy requirement of **section 33(a)** of the Act requires public bodies to have some type of verification procedure, but this is also good business practice for programs that use large personal information systems for delivery of programs or services.

Privacy requirements should be integrated into normal information and systems operations for the program as a whole.

Ensuring accuracy includes making certain that hand-written information used to make decisions, such as clinical notes, is legible.

Retention

Section 33(b) requires public bodies to retain personal information for at least one year after using it to make a decision that affects an individual, so that the individual has a reasonable opportunity to obtain access to it.

This does not include personal information in transitory records if the information is transferred to a different format. This may be the case with records such as counselling notes or notes of an interview panel member that are consolidated into a final document, if it is the policy of the public body to treat these notes as transitory records.

This provision is intended to permit individuals to review and, if necessary, to request correction of information about them that has been used by public bodies before disposition of that information takes place.

Section 33(b) overrides all records retention and disposition schedules by establishing a retention period of one year after use for personal information used in administrative decision-making.

Retain means to maintain custody or control of the personal information. The requirement to retain information means that the information cannot be destroyed, but it could be moved to a records storage facility such as the Provincial Records Centre.

Section 33(b) does not prevent public bodies from storing personal information in another location if the public body can retrieve the personal information in response to a request for access to it.

Public bodies may keep personal information longer than one year, depending on their operational needs and on legal requirements.

7.5 CORRECTION OF PERSONAL INFORMATION

Section 34(1) provides that an individual may request that a public body correct personal information about that individual that is in the public body's custody or control if the individual believes that it contains an error or omission.

This provision applies only to the individual's own personal information. The public body may either correct the information, by changing it or adding new information, or may refuse to correct the information, subject to other provisions discussed below.

An *error* is mistaken or wrong information or information that does not reflect the true state of affairs. An *omission* is information that is incomplete or missing or that has been overlooked.

A public body has *custody* of a record when the record is in the possession of the public body and the public body has a right to deal with the record and some responsibility for its care.

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

See Chapter 1 of this publication for a detailed discussion of custody and control.

Information is personal information if it meets the definition of personal information in **section 1(i)** of the Act, regardless of how a public body comes to have that personal information.

When considering requests for correction of personal information, it is important to distinguish between the two types of information addressed by **section 34**:

- *Factual information* about the individual, such as age, date of birth, income information or qualifications (**section 34(1)**).
- *Opinions* about the individual, such as subjective assessments or evaluations of an individual's condition, abilities or performance (**section 34(1.1)**).

The individual must provide proof in support of the request for correction of factual information. The proof should be of the same nature and at least the same quality as the personal information required when the original collection took place. Examples of documents that might be required to prove facts include a birth or baptismal certificate to prove age, or a notice of assessment from Revenue Canada to prove income.

A public body *must not* correct an opinion (**section 34(1.1)**) including a professional or expert opinion. This provision recognizes that the significance of an opinion may be that it reflects another person's view at the time it was offered, and it may be important to have a record of that view at a later date. The Act allows an individual to have their views about that opinion added to the record for other readers to consider.

Although a public body cannot correct an opinion, it may, in some circumstances, seek or accept another opinion about the individual and reconsider any decision based on the original opinion.

How a Request is Made

In many cases, an individual will ask for personal information to be corrected and supply proof of correction without doing this in a formal way. Public bodies can, and most often will, make corrections without a request under the Act if this is practical and expedites public business.

The formal process for an individual to determine whether or not an error or omission exists in a record is for that individual or a representative to request and review the personal information in accordance with the procedures set out in **Part 1** of the Act.

Where an error or omission exists, in the opinion of the individual, a request for correction can be made to the public body in the form of a letter or on a Request to Correct Personal Information Form.

Requests for correction are subject to the same rules as requests for access under the Act. This includes time limits. It also includes a duty on the part of the public body to fully understand and seek clarification of a correction request.

The Commissioner has the power to review the actions of a public body with respect to requests for correction of personal information.

When a Correction is Made

When a public body accepts a request for correction of an error, all records containing the personal information are corrected. This includes records in all information systems – paper, electronic and microform. Similarly, when a public body agrees to add omitted information, all systems must be updated. The record should be annotated with the date of the correction. A linking mechanism, as described below, may have to be employed when personal information is stored on a medium such as microform, which may be more difficult to update.

To *annotate* personal information is to note the requested correction on the record, close to the information under challenge by the applicant. An annotation should be signed and dated.

When designing electronic forms and databases, care should be given to allow for annotations.

To *link* a record means to attach, join or connect the record to the requested correction. This may consist of a letter or statement from the applicant, or a copy of the Request to Correct Personal Information Form.

When a public body makes an annotation or linkage, it must ensure that the new information is stored and retrieved with the original information whenever the information in question is used for an administrative purpose directly affecting the individual involved. As well, annotations must be made available to the individual should they request access to their personal information.

When a Correction is Refused

Section 34(2) provides that, when a correction is refused or cannot be made, the public body must annotate or link the personal information with that part of the requested correction which is relevant and material to the record in question.

Relevant and material means that there is a direct connection between the correction requested and the use that has been or may be made of the personal information and that the correction is substantive. The correction should be both pertinent to the subject matter and significant in its content.

A public body may refuse or be unable to make a correction that an applicant requests. This may be because the information is not personal information, the applicant has not submitted adequate proof in support of the requested correction, or the information consists of an opinion rather than fact.

In the case of factual information, when the public body is not satisfied with the proof presented, it does not change the information but rather annotates it or links the presented information to the original information.

In the case of an opinion, a public body may describe the information in dispute and place this description, along with a statement that the individual does not agree with the opinion or interpretation, on the record. If practicable, the individual's request for correction may be attached.

Only that part of the requested correction which is relevant to the record being annotated or to which the link is being made is noted. Public bodies are under no obligation to place the applicant's entire request on the record if it contains material that is not germane to the use made of the record.

A public body may use the Annotation Form to set out an annotation relating to a correction that was requested but not made. This form clearly indicates to users that the information has been linked to a correction request and not corrected. It is filed with, or linked to, the information for which a correction was sought.

A copy of this form or equivalent documentation must be sent to the individual requesting a correction at the time that they are informed that the correction is not being made. Any further information supplied by the individual after they received this notice must be filed with the Annotation Form.

If the Annotation Form or the Request for Correction Form cannot be physically attached to the record, a flag may be placed in the file or system containing the personal information in dispute. This will refer a user to a separate file, containing the actual disputed personal information, and indicating that a request for correction or addition of information was made but not granted.

When a public body makes an annotation or linkage, it must ensure that the new information is stored with the original information and will be retrieved whenever the information in question is used for an administrative purpose directly affecting the individual involved. As well, annotations must be made available to the individual should they request access to their personal information

Notification of Other Public Bodies and Third Parties

Section 34(3) obliges public bodies to inform other public bodies, groups of persons, persons, or organizations that have received an individual's personal information from the public body that the applicant has requested a correction or annotation. Notification is required if the personal information has been shared in the year prior to the request for correction.

The notification process ensures that other parties have accurate and complete information for their own decision-making processes.

Section 34(3.1) provides that such notification is not necessary if:

- The correction, annotation or linkage is not material.
- The individual who requested the correction is advised and agrees in writing that notification is not necessary.

This allows public bodies to dispense with third party or public body notification if the correction requested is not required for their decision-making. To ensure that the applicant is advised and agrees with this assessment, consent in writing is required in each instance.

Section 34(4) provides that other public bodies, once notified, must make any correction, annotation or linkage to the relevant personal information disclosed to them and which is in their custody or under their control. This helps ensure that all personal information shared between public bodies is accurate and complete.

Time Limits

Section 34(5) provides that a public body must, within 30 days of receiving the request, give written notice to the individual that either the correction has been made or an annotation or linkage has been made. It is good practice to ensure that other public bodies or third parties are also notified within the 30-day time period.

A public body may extend the time limit to deal with a request for correction for up to 30 days or, with the permission of the Information and Privacy Commissioner, for a longer period.

Section 12 of the Act governs these extensions and the most likely to apply in correction situations are:

- The applicant does not give enough detail to enable the public body to identify a requested record (**section 12(1)(a)**).
- A large number of records is requested or must be searched and responding within the time limit would unreasonably interfere with the operations of the public body (**section 12(1)(b)**).

Pertinent letters are the Acknowledgment of Receipt of Correction Request, Notification Concerning a Request for Correction or Annotation, and Notice to Public Bodies in Receipt of Personal Information.

Transfer of Requests for Correction

Section 34(7) provides authority for a public body to transfer a request for correction of personal information to another public body. This can occur when:

- The other public body originally collected the personal information; or
- The other public body created the record containing the personal information.

This provision ensures that the public body that originally collected or compiled the information deals with a request for the correction of personal information. It can also ensure that all public bodies in receipt of that information are properly notified of the correction. **Section 34(7)** mirrors the provisions for transfer of access to information requests.

If a request is transferred under this section, the public body transferring the request must notify the individual of the transfer as soon as possible. The public body receiving the transferred request has 30 days from the date of the transfer to respond to the request, and can extend this time limit as outlined above.

7.6 PROTECTION OF PERSONAL INFORMATION

Section 35 of the Act requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, disposal or destruction.

Making *reasonable security arrangements* means approving and implementing a security policy for use within a public body.

The policy should address physical, administrative and information technology security. It should be geared to a risk and threat analysis of the information in the custody or under the control of a public body. The policy should assign accountability for carrying out security measures and cover responsibilities and arrangements for protecting personal information. It should also establish requirements for training personnel about appropriate security standards and the application of these to support privacy protection.

The security measures for personal information should be based both on the size of the public body and the results of the risk and threat analysis.

Small public bodies with little personal information in electronic form should concentrate on physical security measures. Larger organizations with sensitive personal information in a variety of forms and media will have to take a wider range of security measures.

The sensitivity of personal information varies widely. For example, some types of medical and financial information have high sensitivity and there is a greater possibility of damage to an individual if they are accidentally disclosed, are stolen or find their way into unauthorized hands in some other way.

Such information requires stringent protection measures, which may include physical access control zones, locked rooms, locked filing cabinets, and personnel reliability checks. Information technology systems may require computer access control codes, automatic tracking of use and telecommunications security devices.

As information systems are implemented that involve more sophisticated technology, security measures should be commensurate with this. For example, data encryption and other privacy-enhancing technologies may be employed.

More routine case files which deal with relatively few elements of personal information, and where the risk of compromise or unauthorized access is low, will require lower grade security measures. These may include locked cabinets, a controlled area that is locked at night, and computers that are kept behind service counters and are accessed through restricted authorization codes.

Public bodies should analyse the types of personal information in their custody or under their control, the varying levels of sensitivity for each type of personal information and the risks and threats that apply to them.

They must take the necessary steps, over time and within available resources, to implement security policies, requirements and procedures relating to the protection of personal information that is sensitive and at risk.

Section 35 also applies to personal information disclosed to or collected or compiled by contractors. Public bodies should ensure that their contracts contain adequate security clauses.

Unauthorized access refers to situations where employees have access to personal information that they do not need to see or handle in the course of their employment. It also refers to situations where members of the public gain access to personal information about other individuals to which they have no right. This may happen through an accidental disclosure or through surreptitious means. Public bodies should have policies in place to verify the identity of those requesting personal information.

Unauthorized collection occurs when personal information is gathered, acquired, received or obtained by any means for purposes that are not allowed under **section 31** of the Act. See the discussion of collection in **section 7.2** of this chapter. This includes collection through interviews, questionnaires, surveys, polls, audio tapes, video tapes, electronic means, forms, telephone calls, and letters.

It is the responsibility of the public body to ensure that personal information is collected in accordance with **sections 31** and **32** of the Act.

Unauthorized use is the use of information for a purpose that is not permitted under **section 36** of the Act. The requirements of this provision are discussed in section 7.7 of this chapter.

The public body is responsible for ensuring that uses of personal information are authorized under **section 36**.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relating the content of personal information in ways that are not permitted under **section 37** of the Act. It includes oral disclosure. The requirements of this provision are discussed in **section 7.8** of this chapter.

The public body is responsible for ensuring that all disclosures of personal information are authorized under **section 37**.

Unauthorized disposal or destruction of personal information means the destruction of records containing personal information in ways that are not permitted under **section 3(e)** of the Act.

Personal information may be at risk of unauthorized disclosure during the disposition process. For example, in other jurisdictions, files containing personal information have been found scattered in the rear of public buildings and left on the hard disks of computers disposed of by a public body.

Destruction of personal information to prevent access by the individuals to whom it refers is unauthorized disposal which is an offence under section 75(1)(e) of the Act.

Most public bodies are subject to the *Archives and Records Act* which says that no record may be destroyed, alienated or transferred to the Public Archives and Records Office except in accordance with a records retention and disposition schedule for those records approved by the Public Records Committee.

For other public bodies, disposal of personal information should occur only in accordance with the by-law, resolution or other policies that approves the storage, transfer or destruction of public body's records (**section 3(e)**).

Examples of unauthorized destruction would be the shredding of information with no authority to do so, the simple discarding of personal information in a garbage container or recycle bin, or the sale of a computer without ensuring that personal information is completely and permanently removed from the hard disk.

The Provincial Records Manager should be consulted for standards relating to the transfer or destruction of records by public bodies.

7.7 USE OF PERSONAL INFORMATION

Section 36 of the Act lists the *only* circumstances under which a public body may use personal information.

These are:

- For the purpose for which the information was collected or compiled or for a use consistent with that purpose (**section 36(1)(a)**);
- If the individual the information is about has identified the information and consented, in the prescribed manner, to the use (**section 36(1)(b)**); or
- For a purpose for which that information may be disclosed under **sections 37, 39 or 40 (section 36(1)(c))**.

Use of personal information means employing it to accomplish the public body's purposes, for example, to administer a program or activity, to provide a service or to determine eligibility for a benefit.

In **section 36(1)(a)**, the *purpose* is the object to be attained by the collection of the information or the thing intended to be done with it. It includes the administration of a particular program, the delivery of a service and other directly related activities.

The *purpose* must conform to **section 31** of the Act, which limits the purposes for which information may be collected. This is discussed in **section 7.2** of this chapter.

Collection must be authorized by an Act or regulation, or it must be for the purpose of law enforcement as defined in **section 1(e)**, or it must be necessary for an operating program or activity of the public body.

The purpose of collection is described in the collection statement provided to the individual when the information is collected directly. When the information is not collected directly, or when it is compiled from several sources, the purpose should be stated in the written policy or procedure dealing with the program.

Information may be *collected or compiled*.

To *compile* information is to draw information from several sources and create a new set of information. It can also mean the creation, calculation, linkage, interpolation or extrapolation of data to produce new information.

A public body may make use of personal information it has gathered, created or manipulated for the specific purposes for which it is permitted to obtain it.

Section 36(1)(a) also permits uses *consistent* with the original purpose. *Consistent use* is defined in **section 38** of the Act as a use that is directly related to the original purpose of collection and that is necessary for performing the statutory duties of the public body.

Section 7.9 of this chapter deals more thoroughly with the concept of consistent uses.

Consent of the Individual

Section 36(1)(b) permits use of personal information if the individual the information is about has identified the information and has consented, in the prescribed manner, to its use.

An individual has *identified* the information means that:

- The individual is aware of the specific information that the public body intends to use.
- The public body has informed the individual about the purpose for which the personal information will be used.
- The public body has informed the individual about any consequences of agreeing or refusing to consent to the use.

Has consented *in the prescribed manner* means that the public body has followed the procedures for obtaining consent set out in **section 6** of the FOIPP Regulations.

This states that consent:

- Must be in writing.
- Must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

Where appropriate, a form or other instrument requesting consent should:

- Indicate the original purpose of the collection, as well as the additional purpose for which the information is to be used and for which consent is being provided.
- Indicate that consent is voluntary.
- Indicate that consent may be revoked at any time.
- To the extent possible, identify any consequences that may result from refusal to consent.
- Indicate the period of time during which the consent remains valid.

A public body may seek consent for a new use of personal information when updating personal information or when collection has to be repeated. The collection statement required under **section 32(2)** should be revised, and use of personal information collected from individuals after that time will be in accordance with the revised purpose.

The different use would be noted at the time of collection, usually on the collection instrument or through pop-up screens for electronic collections. The notification would include the purpose of the collection, a statement that consent is voluntary, identification of any consequences which may result from refusal of consent, and the period of time for which consent will remain valid. Space or opportunity should be provided for the individual to clearly indicate whether or not they give consent to the use.

Approval of a different use by the individual concerned serves as an indication that the person knows the consequences of the use of his or her personal information and has been provided with enough facts to make an informed decision about whether or not to agree to the use.

When the person concerned has not indicated whether or not consent is given to a different use of personal information, public bodies cannot assume the individual has consented.

The absence of consent must be interpreted as the absence of authorization.

Public bodies cannot penalize individuals for refusing to give consent for use for an *additional* purpose by denying them any benefit or service provided through the original collection. Individuals may, however, find they are denied a benefit or service that might have been made available if the individual had consented to use of their personal information for that different purpose.

Section 7.12 of this chapter deals with those classes of persons who may act for minors, incompetent persons, and other individuals in giving or withholding consent.

A Purpose for Which Information may be Disclosed to a Public Body Under Sections 37, 39 or 40

Section 36(1)(c) provides that a public body may use personal information that is disclosed to it by another public body under **sections 37, 39 or 40** of the Act.

Without this provision, a public body would be unable to use personal information disclosed to it in an authorized way. This provision assists in eliminating duplicate collections of personal information by permitting public bodies to use personal information that can be disclosed by another public body under **section 37**.

It also allows a public body to use personal information disclosed to it for research purposes by another public body under **section 39** or by the Provincial Archives and Records Centre or the archives of another public body under **section 40**.

Constraint on Use of Personal Information

Section 36(2) sets some limits on the extent to which a public body can use the personal information in its custody or control.

A public body can use information only to the extent necessary to carry out its purpose in a reasonable manner.

For example, employees in a particular program area who have access to personal information in an electronic database should be provided with access to only those data elements they require to do their job, not to the whole database.

In a reasonable manner means in such a way that a public body is not required to implement overly restrictive procedures on use of personal information when the information is not of a sensitive nature or when disclosure would not be harmful to personal privacy. Severing of information or restricted access to electronic data would be considered on a program-by-program basis.

This statement mirrors the statement covering disclosure of personal information in **section 37(2)**.

It ensures that public bodies to which personal information is disclosed are subject to the same rules as the public body disclosing the information. It is intended to limit disclosure to the minimum amount of information needed to accomplish the purpose of disclosure, and to limit use to the minimum necessary to achieve the purpose of the public body using the information.

7.8 DISCLOSURE OF PERSONAL INFORMATION

Section 37 of the Act lists the *only* circumstances under which public bodies may disclose personal information. It applies to a response to an access request under **Part 1**, or disclosure in the absence of a formal access request.

The word *only* indicates that disclosures of personal information are limited to the specific circumstances outlined in **section 37**. If **section 37** does not provide authority for a disclosure, the public body cannot disclose the information.

Section 37 enables disclosure; it *does not require* disclosure. This is indicated by the word *may* in the introduction to the section. Public bodies should look at the circumstances surrounding each request when deciding whether to disclose personal information. They should also disclose only the information pertinent to the request.

Section 37(2) states that a public body may only disclose personal information that is reasonably required to carry out the purposes described in the immediately preceding subsections. These purposes are described in the following pages. Disclosure has to be carried out in a reasonable manner (see section 7.7 of this chapter).

Public bodies should be careful to disclose only limited amounts of personal information. They have a responsibility in most cases to clarify and understand the reasons for the request for disclosure. Disclosures should be made in a way that helps the requester and is cost-effective for the public body. This may mean that not all disclosures are in writing, or that, when a working relationship has been established, all the proofs required are not asked for each time a request is made.

Disclose means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or give personal information by any means to someone. It includes oral transmission of information by telephone or in person; provision of personal information on paper, by facsimile copy or in another format; and electronic transmission through electronic mail, data transfer or the Internet. The disclosure may be made:

- To the person whose information it is, either in response to a routine request for information or in response to a FOIPP request;
- To an individual's personal representative who is entitled to exercise the rights of that individual under **section 71** of the Act;
- To any other person in response to a FOIPP request, as a release in the public interest, when the disclosure would not be an unreasonable invasion of privacy, or when **section 37** of the Act specifically allows the disclosure; or
- To other public bodies, to legislative, legal and judicial officers, to other levels of government, or to non- government organizations. These disclosures may take place to support the activities of either the public body disclosing the information or the party to which it is disclosed.

Public bodies should keep a record of any disclosures of personal information made under **section 37**. This may consist of a note on a file or a flag in an electronic system that refers to a paper record or another data file. A record of disclosures is needed to enable a public body to comply with its obligation under section 34(3) to inform anyone to whom it has disclosed personal information of any correction to that information.

Such records of disclosure should include:

- The name of the individual whose personal information is requested.
- The nature of the requested information and the purposes for which it will be used
- The authority for the request.
- The title, business address and business telephone number of the contact person in the requesting public body or agency.
- The name and signature of the officer or employee of the public body who authorizes the use or disclosure.

Public bodies must have appropriate administrative controls in place to ensure against the disclosure of personal information to anyone who is not permitted access to the information under the provisions of the FOIPP Act.

Public bodies should regularly review their disclosure policies and practices to ensure that they meet the requirements of the Act. Where it is found that disclosures are not authorized, practices should be altered to meet legal requirements or discontinued.

Section 37 does not prevent the routine disclosure of an individual's personal information to that individual if the public body has adopted a policy of disclosing that category of personal information. In these circumstances, the public body will provide the personal information without a FOIPP request.

In the following pages, each permitted disclosure is outlined and discussed.

In accordance with Part 1 of the Act (section 37(1)(a))

This provision permits disclosure to respond to access requests and to comply with the public interest provisions of the Act. A disclosure may take place when:

- An applicant has requested access to their own personal information, subject to the exceptions in **sections 14 to 27** and the paramountcy provision in **section 5**;
- An applicant has requested access to records containing personal information about another individual and disclosure of the personal information does not constitute an unreasonable invasion of the privacy of the other individual under **section 15**, subject to other exceptions and to third party notification requirements; or
- **Section 30** applies.

Disclosure would not be an Unreasonable Invasion of a Third Party's Privacy Under Section 15 (section 37(1)(a.1))

This provision permits disclosure when it is clear that the personal information would not be excepted under **section 15**. It is intended to permit disclosure of personal information described in **section 15(4)** without the necessity of a FOIPP request.

This provision gives public bodies more flexibility in responding to requests for personal information that clearly would be provided if a FOIPP request were made. It allows for a more helpful and timelier response to such requests.

When another provision of **section 37** permits disclosure, the disclosure should be made under that provision. Examples are: disclosure with the consent of the individual, disclosure required or authorized by an Act of Prince Edward Island or Canada, and disclosure for research purposes.

In some circumstances, public bodies will be able to establish policies and practices for routine disclosure in response to requests for particular classes of personal information. In establishing such policies, public bodies should determine whether any of the other exceptions outlined in **Part 1** of the Act might apply to the information.

Examples of classes of personal information for which a policy might be appropriate include:

- Information about employee classification, salary range, employment responsibilities and discretionary benefits (**section 15(4)(e)**).
- Financial and other details of a contract to supply goods or services (**section 15(4)(f)**).
- Information regarding permits or licences relating to commercial or professional activities or real property (**section 15(4)(g)**).
- Details of discretionary benefits of a financial nature (**section 15(4)(h)**).
- Personal information about an individual who has been dead for 25 years or more (**section 15(4)(I)**).

Public bodies may charge a fee for such information.

For more information on **section 15(4)**, see Chapter 4.4 of this publication.

Original and Consistent Uses (section 37(1)(b))

This provision permits disclosure for the purpose for which the information was collected or compiled or for a purpose consistent with that purpose.

The *purpose* for which personal information was collected or compiled means the object to be attained or the thing intended to be done. Generally, that is the administration of a program or the provision of a service. Such purposes must conform to **section 31** of the Act, which limits the purposes for which information may be collected. This is discussed in section 7.2 of this chapter.

Personal information is *compiled* when it is assembled from several sources or generated, calculated, extrapolated, interpolated, linked, deduced, or otherwise created. The word implies collection from more than a single source and not directly from an individual.

A *consistent use* is one that has a direct and reasonable connection to the original use and that is necessary for performing the statutory duties of, or for operating an authorized program of, the public body (**section 38**). A disclosure is therefore permissible if it is a logical extension of the original use.

Examples of consistent uses include:

- Providing a list of participants in a program to another part of a public body for evaluation of the program.
- Using the assessment roll to confirm property ownership when needed for other municipal purposes.
- Disclosing information to another public body which is carrying out a part of the program for which the personal information was originally collected.

A more detailed explanation of *consistent use* is provided in section 7.9 of this chapter.

Consent to Disclosure (section 37(1)(c))

This provision permits disclosure of an individual's personal information when the individual has identified the information and consented, in the manner prescribed in **section 6** of the FOIPP Regulations, to the disclosure.

The individual has *identified* the information means that the public body has informed the individual about:

- The specific information that the public body intends to disclose.
- The purpose for which the personal information will be disclose.
- Any consequences of agreeing or refusing to consent to the disclosure.

Consent for a disclosure should be sought as early as possible after the need has been identified. Ideally, it should be sought at the time the information is collected. In such cases, the request for consent to disclose is added to the collection instrument, indicating:

- To what public body, group or organization the information may be disclosed.
- That consent to disclosure is voluntary, noting any consequences that may result from refusing to consent to the disclosure.
- The period for which the consent will remain valid.

The same procedure for obtaining and recording consent to disclosure may be used when personal information is collected for an administrative process that will be periodic and ongoing.

In the case of electronic collection, pop-up screens can be used to provide notification to the individual, provide the requisite explanations and enable consent or refusal. In all instances, space or opportunity should be provided for the individual to clearly indicate whether consent to the disclosure is given.

Section 6 of the FOIPP Regulations states that consent under **section 37(1)(c)** must:

- Be in writing.
- Specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

The absence of consent is interpreted as the absence of authorization. When the person concerned has not indicated any consent to disclosure of personal information, and no other provision exists to permit disclosure, public bodies cannot disclose information.

A public body must not penalize an individual for refusing to consent to a disclosure of personal information for a purpose other than the purpose for which the personal information was collected. A public body must not deny the individual the benefit or service for which the personal information was originally collected.

Consent may be given by a representative acting on behalf of an individual in accordance with the conditions set out in **section 71(1)**. These conditions are discussed in detail in section 7.12 of this chapter.

Examples of consent to disclosure include: agreement to have references provided in support of job applications; agreement to provide information to Revenue Canada in order to obtain income verification from that source; consent to disclosure in response to third party notice under **section 28** and agreement to the use of photographs for promotional purposes.

Disclosure to Comply With an Enactment of Prince Edward Island or Canada or With a Treaty, Agreement or Arrangement (section 37(1)(d))

This provision permits disclosure of personal information to comply with an Act of Prince Edward Island or Canada, a regulation made under such an Act, or with a treaty, arrangement or agreement made under either an Act or a regulation. It does not apply to the legislation of other provinces, territories or foreign states.

Public bodies should prepare a list of all agreements, arrangements and treaties, as applicable, under which they disclose personal information.

Disclosure to *comply with an enactment of Prince Edward Island or Canada* means disclosure of personal information as *required* by either provincial or federal legislation. The enactment must impose an obligation to disclose the personal information.

Disclosure to *comply with a treaty, arrangement, or agreement* made under an enactment of Prince Edward Island or Canada means disclosure of personal information as *required* by the treaty, arrangement or agreement.

The enactment must provide authority for the provision in the treaty, arrangement or agreement, and that provision must specifically authorize disclosure of the personal information.

A *treaty* is a formally concluded and ratified agreement between or among independent states. Only the federal government of Canada has the power to conclude treaties with foreign countries.

An *arrangement* is a coming to terms on how certain matters will be conducted. Arrangements should, whenever possible, be in writing. A verbal arrangement should be allowed only in very exceptional circumstances, such as sensitive law enforcement, security or intelligence matters, and only at the insistence of one or more of the parties. Where an arrangement is unwritten, disclosures should be approved at a senior level within the public body.

An *agreement* is similar to an arrangement but is more precise in setting out the actions to be taken. *All agreements should be in writing.*

Agreements concerning the disclosure of personal information by public bodies to other organizations, including federal, provincial, municipal, and foreign governments and international bodies, should contain:

- A description of the personal information to be shared.
- The purposes for which the information is to be shared and used.
- A statement of all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially with respect to its use and disclosure.
- A statement specifying whether information received by a public body will be subject to the provisions of the FOIPP Act or, for other jurisdictions where comparable legislation exists, whether that legislation will apply.
- A statement that the sharing of the personal information shall cease if the recipient is discovered to be improperly disclosing the shared information.
- The names, titles and signatures of the officials in both the supplying and receiving public bodies who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.

Disclosure in accordance with an enactment of Prince Edward Island or Canada that authorizes or requires disclosure (**section 37(1)(e)**): This provision is related to **section 37(1)(d)**. However, whereas in **section 37(1)(d)** disclosure must be *for the purpose of complying* with an enactment, and is therefore likely to be required by law, in **section 37(1)(e)**, disclosure is permitted if it is either required or *authorized* by an enactment of Prince Edward Island or Canada. If disclosure of personal information is authorized – but not required – by an enactment, the head of the public body has more discretion as to whether or not to disclose the information.

Complying with a Subpoena, Warrant or Order (section 37(1)(f))

This provision permits personal information to be disclosed in order to comply with legal processes that require the production of information. These processes include the use of a subpoena, warrant or order issued or made by a court, person or body **having jurisdiction in Prince Edward Island** to compel the production of information or with a rule of court **binding in Prince Edward Island** that relates to the production of information.

A *subpoena*, also called a “summons to witness,” is a command issued by a party in litigation requiring the attendance of someone as a witness at a court or hearing. It will specify a certain place and time when testimony on a certain matter will be required, and may also order a person to meet the requirements of a court to disclose information.

Time is usually of the essence in dealing with a subpoena, as it is often served with very little notice. Public bodies cannot ignore subpoenas since they would risk being cited for contempt of court and, at a minimum, fined.

A *warrant* is a judicial authorization to collect information – in this context, personal information.

An *order* is an authoritative command, direction or instruction to produce something – again in this context, personal information.

Although **section 37(1)(f)** is permissive in nature, public bodies normally comply with orders, warrants or subpoenas because they are required by law to do so and generally wish to assist the administration of justice.

Public bodies should consult their legal advisor when they receive an order, warrant or subpoena in order to determine whether it refers to information that is actually in the custody or under the control of the public body, whether the instrument has been served properly and whether there is some compelling reason to oppose the order, warrant or subpoena.

To an Officer or Employee of the Public Body, or to a Member of Executive Council (section 37(1)(g))

This provision permits disclosure to officers or employees of the public body that has custody or control of the personal information and to Cabinet members. It *does not* allow disclosure to employees or officers of *other* public bodies.

An *employee* is a person employed by a public body. The definition in **section 1(c)** of the *Act* includes a person retained under contract to perform services for the public body.

The term *officer* is included to ensure that all persons working for a public body in any capacity are encompassed by the provision.

A member of the Executive Council includes the President of Executive Council and a Minister.

The provision does not allow an official or employee or member of the Executive Council automatic access to all personal information within a public body. The test for disclosure is whether the information is *necessary for the performance of duties*. Disclosure is permissible only if access to the particular personal information is needed to do a job or deal with a particular situation. The persons to whom the information is disclosed should be able to prove a need to see, generate or handle the personal information in order to do their jobs.

Examples of cases where disclosure might be necessary for the performance of an employee's duties include the following:

- A staffing team requires access to the resumes of applicants in order to carry out the recruitment function.
- A service counter team needs to be informed if a client has a history of acting violently when interacting with departmental staff and if there is a need for extra security when the individual approaches the office.
- A Minister needs background information about an issue and the people they are meeting in order to understand the problem and their needs.

For the Delivery of a Common or Integrated Program or Service (section 37(1)(g.1))

This provision has the same requirements as **section 37(1)(g)**, but permits disclosure to officers or employees of *another* public body. This is permitted when two or more public bodies are working together to provide or deliver a common program or service.

Section 37(1)(g) does not allow disclosure to an organization that is not a public body.

Common means that there is a single program or service that is provided or delivered by two or more public bodies.

Integrated means that the program has several distinct components, each of which may be provided or delivered by separate public bodies, but those components together constitute the program or service.

This provision allows for the sharing of personal information between the service providers in order to deliver the service to the clients. A common client does not, of itself, meet this definition.

Factors that will determine whether or not a program or service meets the definition include:

- Evidence of joint planning.
- A formal agreement or legislative authority for working together.
- Common goals expressed by the partners.
- Evidence of collaboration or cooperation in delivery.

When public bodies are implementing such programs or services, they should:

- Ensure that individuals participating in the program are notified of all the partners and of the sharing of personal information.
- Disclose information in non-identifiable form whenever possible.
- Disclose personal information only to those who need to know about a particular individual.
- Disclose personal information only to the extent necessary for program or service delivery.
- Ensure that personal information is not used for any other purpose.

To Enforce a Legal Right of the Government of Prince Edward Island or a Public Body (section 37(1)(h))

This provision permits the disclosure of personal information to enforce a legal right that the Government of Prince Edward Island or a public body has against any person.

In most cases, the disclosure of personal information under this provision will be to the legal representatives of a public body or to the Office of the Attorney General as the provincial government's legal representative. The legal rights may relate to civil or criminal law.

Collecting a Fine or Debt or Making a Payment (section 37(1)(I))

This provision permits disclosure of personal information to:

- Collect a fine or debt owing to the Government of Prince Edward Island or a public body or an assignee of either of them; or
- Make a payment owing by the Government of Prince Edward Island or a public body.

This provision enables public bodies to exchange personal information with other public bodies and outside agencies to locate an individual and collect a fine or debt or in order to make a payment.

It *does not* permit information to be exchanged between public bodies for the purpose of determining whether a fine, debt or a benefit is owed. This decision must be made before the information is disclosed.

The provision permits disclosure to a private collection agency to which the debt has been assigned. It does not permit disclosure to assist such a collection agency, or any other person or organization that is not a public body, to collect a debt owed to a person or organization that is not a public body.

Documentation requesting disclosure under this provision should be in writing and specify:

- The nature of the information to be disclosed.
- The name of the public body, person or organization receiving the information.
- Any other necessary identifying information such as a case or file number.
- The purpose of the request, including a citation of the legal authority for collecting the fine or debt.
- The name, title and business address of the official making the decision to disclose.

The information disclosed should be the minimum needed to enable the collection or payment to be made. Usually this will be the name, last known address and telephone number, and any contact information provided by the individual. Disclosure should always be in writing.

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a by-law.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

This provision is intended to assist public bodies in cases where their legislative mandate does not specifically extend to the collection of fines and debts. It gives them an authority under which to pursue these activities. Many public bodies already have authority to collect fines and debts in their legislation.

Determination or Verification of Suitability or Eligibility for a Program or Benefit (section 37(1)(j))

This provision permits the disclosure of personal information to determine an individual's suitability or eligibility for a program or benefit, including verifying continued eligibility for the program or benefit.

Section 37(1)(j) allows personal information to be disclosed when there is a need to determine whether or not an individual meets the eligibility or suitability criteria for a particular program or benefit. The information must have been collected or compiled by a public body. Disclosure may be made to any organization or institution that needs such verification information; it is not limited to another public body.

Normally, disclosure will only be made after an application has been made by an individual to participate in a program or for a benefit. Public bodies collecting such information should comply with the guidelines set out in section 7.3 of this chapter.

Eligibility means the state of being qualified or permitted to be chosen for a program or benefit.

Suitability means the characteristics of an individual that enable them to be chosen for a program or benefit. Examples of disclosures that might be permitted under this provision include:

- Verification of employment information when someone applies for employment insurance or employment counselling.
- Disclosure of information from a seniors' lodge to a health authority to determine suitability for nursing home care.
- Confirmation of membership in a library when an individual uses their library card in another library.
- Provision of information on attendance or marks to enable a second year of grant support to a student.

Audit Purposes (section 37(1)(k))

This provision permits the disclosure of personal information to the Auditor General and to other persons and bodies established by regulation for audit purposes.

The *Auditor General* is an Officer of the Legislature appointed by the Lieutenant Governor in Council. The role of the Auditor General is to examine the accounts and records of the Government relating to the consolidated revenue fund and all public money, including trust and special funds under the management of the Government and relating to public property. The Auditor General must report annually to the Legislature on their work, including findings as to whether or not departments and public bodies have carried out their financial responsibilities. This provision does not apply to the Auditor General of Canada.

For audit purposes means for the purposes of the examination of accounts, including value-for-money audits that examine revenues, expenditures and public policy approaches. It does not include the verification of a claimant's eligibility for a program, benefit or service, where an actual decision would be taken about an individual.

The persons to whom personal information may be disclosed for audit purposes are specified in **section 7** of the FOIPP Regulations. Disclosure can be made to persons who are employees of a public body, including a person retained under contract to perform services for the public body. Personal information may be disclosed in order to carry out a financial or other formal and systematic examination or review of a government program or activity or a portion of a program or a activity that includes personal information.

Such an audit must be sanctioned by statute, regulation or public policy relating to the public body.

When a contractor is hired to conduct an audit requiring disclosure of personal information under this provision, the contractor should be advised of, and agree to abide by, the provisions of the FOIPP Act, as well as policy relating to the protection of privacy under the FOIPP Act.

Information disclosed under **section 37(1)(k)** is only to be used for audit purposes and not for operational or administrative purposes involving the individuals concerned.

Examples of disclosures that may be permitted under this provision include:

- Disclosure to an accounting or audit firm engaged to conduct a financial audit of a public body.
- Disclosure to a person auditing methods of determining how a housing management body determines eligibility for low income housing.
- Disclosure for personnel audits, such as classification reviews or quality assurance audits of the work being performed.

Disclosure to a Member of the Legislative Assembly (section 37(1)(l))

This provision permits disclosure of personal information to a Member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem.

A Member of the Legislative Assembly (MLA) is a person elected as a representative of a constituency within the province of Prince Edward Island to represent the interests of the voters in that constituency in the Legislative Assembly.

This provision permits disclosure only to Members of the Legislative Assembly of Prince Edward Island, not to those working for them, and only to assist the person concerned to resolve a problem.

The provision *does not* permit the disclosure of personal information to federal Members of Parliament. These representatives may, however, obtain personal information about an individual with their consent.

The purpose of disclosure under **section 37(1)(l)** must be to *assist in resolving a problem*. This includes helping an individual to provide information to a public body, inquiring about decisions or about a service or benefit, or correcting a mistake or misunderstanding. Where resolution of the problem is relatively straightforward, the public body can discuss the issue with the MLA and, with their agreement, simply call the individual concerned and provide the information directly.

The written consent of the individual concerned is not normally necessary for disclosure to MLAs under this provision.

However, it is good practice to obtain the written consent of the individual in order to specify what personal information is to be disclosed to the MLA.

It is likely that the MLA will pass the personal information they receive from a public body to the person concerned. Public bodies should bear in mind the exceptions to the right of access set out in Part 1 of the Act when deciding what it is and is not appropriate to disclose under this provision.

Representative of a Bargaining Agent (section 37(1)(m))

This provision permits disclosure of personal information to a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry.

This provision permits disclosure to a representative of a union or other organization that negotiates on behalf of workers with their employers for improvements in pay, hours, benefits, and other working conditions, and that works to protect the rights of employees.

The individual must sign and date a statement of authorization or representation clearly stating to whom the information may be disclosed and for what purpose. Disclosure is limited to personal information that is necessary for the purpose of *making an inquiry* and the representative may receive only that personal information that the employee has specifically authorized for release.

The representative, unless duly authorized as the employee's representative, may not exercise the employee's right of access to the rest of their personal information. Nor can they exercise the right to request correction of the employee's personal information.

Public bodies should ensure that their employees understand the purposes of the Act with respect to protection of personal information and the way the Act is applied in circumstances where a bargaining agent requests information about an employee.

Disclosure for Archival Purposes (section 37(1)(n))

This provision permits disclosure of personal information to the Public Archives and Records Office or the archives of a public body for permanent retention.

This provision does not permit disclosure to private archives such as those run by a private museum or historical society.

This provision is permissive in nature. It permits the disclosure of personal information to personnel of the Public Archives and Records Office or the archives of a public body:

- During the scheduling process to determine what personal information may have long-term archival and historic value.
- After the transfer and deposit of the personal information in the Public Archives and Records Office or the archives of a public body for on-going research purposes.

Further disclosure by archives is governed by **section 40** of the Act. See section 7.11 of this chapter for a discussion of **section 40**.

Assistance to Law Enforcement (section 37(1)(o))

This provision permits the disclosure of personal information to a public body or a law enforcement agency in Canada to assist in an investigation:

- Undertaken with a view to a law enforcement proceeding; or
- From which a law enforcement proceeding is likely to result.

Law enforcement is defined in **section 1(e)** of the Act and further explained in Chapter 4.7 of this publication.

A *law enforcement agency in Canada* includes a variety of agencies that are responsible for enforcing statutes. Examples of such agencies are the Office of the Attorney General, the RCMP, provincial or municipal police services, and Revenue Canada.

Public bodies should not disclose personal information when the law enforcement agency cannot provide definite and focussed investigative information as to why disclosure is needed. Personal information should not be disclosed on the basis that there is a suspicion, surmise or guess that it may be useful to an investigation.

A request by a law enforcement agency for personal information should be in writing and should be retained by the public body as a record of whether or not the disclosure occurred.

Public bodies should ensure that requests for personal information from law enforcement agencies are justified and contain:

- The name of the individual whose information is requested.
- The exact nature of the information desired.
- The authority for the investigation.
- The purpose for which the requesting agency will use the information.
- The name, title and address of the person authorized to make the request.

The FOIPP Act is not intended to impede authorized law enforcement activities or to prevent the sharing of personal information for the purposes of law enforcement investigations and proceedings. The Act is intended to ensure that law enforcement agencies and other public bodies operate under a consistent set of rules. These rules appear in a number of different contexts throughout the Act.

Law enforcement agencies are encouraged to use the Law Enforcement Disclosure Form or a similar form when requesting disclosure of personal information. The record of disclosure should normally be kept in a separate file that documents all requests for disclosure from law enforcement agencies, since this record may itself qualify for exception under **section 18** of the Act.

An *investigation* is a methodical process of examination, inquiry and observation. Examples of investigations include the examination of crime scenes, the interviewing of witnesses and the amassing of evidence, all of which tend to generate recorded information on the matter under investigation.

To use this provision, the investigative process must be with a view to, or likely to lead to, law enforcement proceedings. However, there does not have to be a guarantee that the proceedings are actually going to occur and, indeed, they could be suspended for many reasons, including lack of evidence.

Proceeding means an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions concerning a person's rights. In this context, it includes administrative proceedings before agencies, boards and tribunals if the proceedings could lead to a penalty or sanction, including a penalty or sanction imposed by another body to which the results of the proceeding may be referred.

A *law enforcement proceeding* has as its purpose the imposition of penalties or sanctions, as opposed to the gathering of information for criminal or security intelligence purposes.

Section 37(1)(o)(ii) limits the discretion to disclose personal information with the requirement that, at a minimum, the disclosure of personal information must be to assist an investigation from which a *law enforcement proceeding is likely to result*. When disclosure is contemplated before an actual law enforcement proceeding is under way, there must be a probability that a law enforcement proceeding will go forward.

Disclosure among law enforcement agencies (section 37(1)(p))

This provision permits a public body that is a law enforcement agency to disclose personal information:

- To another law enforcement agency in Canada; or
- To a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

This provision permits law enforcement agencies in Prince Edward Island to exchange personal information with their federal, provincial and municipal counterparts in Canada. Examples include the RCMP, provincial securities commissions and other police services.

As well, the provision deals with *law enforcement agencies in foreign countries*. This includes police forces and other law enforcement organizations in other countries, international law enforcement organizations and municipal and state police forces in foreign countries. Examples would be the Metropolitan Police in England, the Federal Bureau of Investigation and the United States Immigration and Naturalization Service in the United States, and Interpol.

Disclosures under **section 37(1)(p)(ii)** must be made in accordance with an arrangement, written agreement treaty or legislative authority. The same conditions for an arrangement, agreement or treaty prevail as for **section 37(1)(d)** described above.

Legislative authority means a statute, regulation or other legislative instrument.

Notification in Case of Injury or Sickness (section 37(1)(q))

This provision permits disclosure of personal information so that a spouse, relative or friend of an injured, ill, or deceased individual may be contacted.

It would also allow disclosure of such personal information as whether the individual has been taken to a hospital or requires assistance to get home.

In Accordance with Sections 39 or 40 (section 37(1)(r))

This provision permits the disclosure of personal information for research and statistical purposes. The conditions applicable to research disclosures are discussed in sections 7.10 and 7.11 of this chapter.

Disclosure to an Expert Under Section 16(2) (section 37(1)(s))

This provision permits disclosure of personal information to an expert as provided for in **section 16(2)** of the Act. It allows the expert to determine whether or not release of the applicant's own information to the applicant could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

Section 5 of the FOIPP Regulations establishes conditions for such disclosure of personal information to a physician, chartered psychologist, psychiatrist or other expert as follows:

- The public body may disclose information relating to the mental or physical health of an individual to a medical or other expert for an opinion on whether disclosure of this information could reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health.

- A medical or other expert to whom information is disclosed must not use the information except for the purposes of determining the harm described above.
- The public body must require a medical or other expert to whom the information will be disclosed to enter into an agreement relating to the confidentiality of the information.
- If a copy of the record containing information relating to the mental or physical health of an individual is given to a medical or other expert for examination, the medical or other expert must, after giving the opinion, return the copy of the record to the public body or dispose of it in accordance with the agreement between the public body and the expert.

Court or Quasi-Judicial Proceedings (section 37(1)(t))

This provision permits disclosure of personal information for use in a proceeding before a court or quasi-judicial body to which the Government of Prince Edward Island or a public body is a party.

It permits the disclosure of personal information to the legal representatives of the Government of Prince Edward Island or a public body for use in such proceedings. It also permits disclosure to the members of the quasi-judicial body or court.

Disclosure is normally to, or through, the legal representative of the public body which represents the public body in legal matters. In the case of a government department, such a disclosure would usually be to the Office of the Attorney General as the legal representative. Such information may be disclosed to the legal representative of the other parties to a proceeding in accordance with the court disclosure and discovery rules that apply.

For more information about quasi-judicial bodies see Chapter 1.7 of this publication.

Disclosure to a Place of Lawful Detention (section 37(1)(u))

This provision permits the Attorney General or an agent or lawyer of the Attorney General to disclose personal information in the custody or under the control of that department. The information may be disclosed to a place of lawful detention in order to provide for the appropriate supervision of any individual detained in custody.

Management of Personnel (section 37(1)(v))

This provision allows government departments and public bodies subject to the *Civil Service Act* to disclose personal information about an employee or prospective employee to each other. The provision recognizes the provincial government as the employer for all provincial departments.

The provision allows other public bodies to disclose the same kind of information only *within* the public body that has custody and control of the information.

No disclosure is permitted to other public bodies or the private sector without the written consent of the individual unless some other provision of section 37 permits it.

Management or administration of personnel includes all aspects of the management of human resources of a public body. This includes staffing, job classification, recruitment and selection, salary and benefits, hours and conditions of work, leave management, performance review, training, separation and layoff.

Employees should be informed, in a general way, of how they should expect their personal information to be collected, used and disclosed within the personnel management system.

Disclosure of personal information for the purposes of the management or administration of consultant, professional or other personal services contracts should be addressed in the terms of the contracts.

Disclosures under this provision are permitted only within the official framework that governs the management and administration of personnel within a public body or across the Government of Prince Edward Island.

Enforcement of Maintenance Orders (section 37(1)(w))

This provision permits the disclosure of personal information about individuals for the purposes of enforcing a maintenance order under the *Maintenance Enforcement Act*.

Public bodies should disclose only personal information that is relevant to the enforcement process relating to the order.

Disclosure can take place only to the Director of Maintenance Enforcement or someone delegated to act on their behalf.

NEW (37 (1)(w.1) to the Public Trustee appointed under the *Public Trustee Act* R.S.P.E.I. 1988, Cap. P-32.2, for the purpose of managing the estate of a person under the *Public Trustee Act*;

Disclosure to an Officer of the Legislative Assembly (section 37(1)(x))

This provision permits the disclosure of personal information to an Officer of the Legislative Assembly if the information is necessary for the performance of the duties of that officer. Officers of the Legislative Assembly are the Auditor General, the Clerk, Clerk Assistant and Sergeant-at-Arms, the Chief Electoral Officer, the Information and Privacy Commissioner and the Conflict of Interest Commissioner (**section 1(h)** of the Act).

Disclosure under **section 37(1)(x)** is restricted by the requirement that the information is necessary for the performance of the duties of the Officer of the Legislative Assembly.

If the reason for the disclosure is not clear from the request, public bodies should seek an explanation as to why the personal information is needed.

Information may be disclosed under this provision for the purpose of a review of a privacy complaint by the Information and Privacy Commissioner.

Supervision of an Individual by a Correctional Authority (section 37(1)(y))

This provision permits the disclosure of personal information about an individual for the purpose of supervising the individual while they are under the control or supervision of a correctional authority.

Supervision includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of individuals held in a correctional institution.

Disclosure of Information Available to the Public (section 37(1)(z))

This provision permits personal information to be disclosed when that information is available to the public. It applies to information that has been published in any form or which constitutes or is a part of a record that is publicly available.

The provision covers situations where a public body wishes to obtain personal information that is in the public domain from another public body, as well as disclosure to the public or to a private-sector organization.

It is important, however, to assess carefully just how public the information is. For example, just because personal information about an individual has been published in the media does not mean that the information should automatically be treated as public and disclosed freely. If a public body is contemplating making this type of disclosure, it should take into consideration the possibility that the individual involved might still find such disclosure an unreasonable invasion of their privacy.

Examples of public information that might be disclosed under this provision include:

- Individual employee information in a corporate telephone directory available for purchase or freely available on the Internet.
- Biographical information about board appointees published in a newsletter
- Information in court decisions published in law reports.

Routinely Disclosed in a Business Card or Professional Context; Section 37(1)(z.1)

This provision permits disclosure of an individual's name, business information as defined but does not permit the disclosure of other personal information about an individual or personal information about anyone else.

Disclosure to a Relative of a Deceased Person (section 37(1)(aa))

This provision permits personal information to be disclosed to a relative of a deceased individual if that disclosure is not an unreasonable invasion of the deceased individual's personal privacy.

Privacy for a deceased individual normally endures for a period of 25 years (see **section 15(4)(i)**).

Section 37(1)(aa) permits a public body to disclose information earlier to a relative. A *relative* in this context means a spouse, child, parent, sibling, or anyone else that can prove a family relationship with the deceased.

Evidence of the relationship of the person to the deceased individual should be produced before personal information is disclosed. This should consist of reliable documentation of the relationship (e.g., a birth or marriage certificate). As well, if a public body is not certain that the individual is deceased, the person seeking disclosure must provide reliable evidence that the individual is dead (e.g., a death certificate or obituary).

This provision recognizes that the privacy interests of an individual generally diminish with the passage of time, and that there may sometimes be a need for relatives to have access to information about deceased family members to resolve personal matters or advance individual rights.

The constraining factor in the provision is the *unreasonable invasion of privacy* test relating to the deceased individual. In considering disclosure, the public body should weigh the sensitivity of the information against the interest of the relative in having access to the information. The need of the relative should go beyond mere curiosity about the deceased individual. For more information on making a decision, see Chapter 4.4 of this publication.

Particularly important factors to consider are whether:

- The personal information was supplied in confidence.
- The disclosure is desirable for the purpose of subjecting the activities of the Government of Prince Edward Island or a public body to public scrutiny.
- The personal information is relevant to a fair determination of the requesting individual's rights.
- The personal information was originally supplied by the requesting individual.
- Disclosure may endanger the physical or mental well-being of any other living member of the family.
- There are grounds to believe that another member of the family does not want the information disclosed to the relative.
- The personal information is likely to be inaccurate or unreliable.
- The information contains medical, psychological or social work case reports or data which it is reasonable to believe would prove harmful to familial relationships.
- Disclosure may harm the reputation of the deceased, who cannot defend themselves.

Legal Representative of Inmate (section 37(1)(bb))

This provision permits the disclosure of personal information to a lawyer or articulated clerk who is acting for an inmate under the control or supervision of a correctional authority.

For information on *supervision* see the discussion on **section 37(1)(y)** above.

Disclosure to Avert Danger to Health or Safety (section 37(1)(cc))

This provision permits disclosure when a public body has reasonable grounds to believe the disclosure will avert or minimize a serious health or safety risk to any person. The danger has to be imminent.

Imminent danger means a danger that is likely to arise immediately or very soon.

A public body will have to consider all the information in its possession about an individual when making a decision. Past behaviour of the individual is one factor that may assist in decision-making.

An example of information that might be disclosed under this provision is information about the escape or release of a violent offender to a past victim.

7.9 CONSISTENT USES

Section 38 of the *Act* provides that for the purposes of **sections 36(1)(a)** and **37(1)(b)**, a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure:

- Has a reasonable and direct connection to that purpose.
- Is necessary for performing the statutory duties of or for operating a legally authorized program of, the public body that uses or discloses the information.

Section 38 balances the protection of individuals' privacy against the need of public bodies to use and disclose personal information effectively to carry out program activities and fulfil their legislated mandates.

Section 36(1)(a) allows a public body to *use* personal information for a purpose that is consistent with the purpose for which the information was originally collected. In most cases the public body using the information will be the public body that collected it. However, if the personal information has been collected for the purposes of delivering a common or integrated program or service, the public body using the information may not be the public body that originally collected it.

See section 7.8 of this chapter for further information on common or integrated programs and services (**section 37(1)(g.1)**).

Section 37(1)(b) allows a public body to *disclose* personal information for a purpose that is consistent with the purpose for which the information was originally collected. In most cases this provision will apply to disclosure outside the public body.

The new use or disclosure must be consistent with the purpose for which the information was collected or compiled.

A use or disclosure has a *reasonable and direct connection* to the original purpose if there is a logical and plausible link to the original purpose. A new use should grow out of or be derived from the original use.

A use or disclosure is *necessary for performing the statutory duties of, or for operating a program of, the public body* if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed.

A consistent use or disclosure must meet both of the above conditions to be valid.

Examples of Use for Consistent Purpose

Evaluation of a program

Public bodies will have a regular need to evaluate the operation and success of their programs. This is particularly true of new programs or those that have changed in some way. This provision allows a public body to select clients or participants who can participate in that evaluation through questionnaires or interviews.

Verification of ownership

Public bodies issue permits for such things as development of a property, demolition and burning. These permits are issued to the owner of a property. This provision allows staff who approve the permit to verify ownership from the assessment roll.

Expansion of a program

Public bodies set criteria for participation in programs. If the criteria are broadened, people who were originally rejected may become eligible. This provision allows a public body to determine eligibility on the basis of the original submissions from these people rather than collecting the information again.

7.10 DISCLOSURES FOR RESEARCH OR STATISTICAL PURPOSES

Section 39 of the Act enables a public body to disclose personal information for a research purpose, including statistical research, only if:

- The research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Information and Privacy Commissioner.
- Any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest.
- The head of the public body has approved conditions relating to the following:
 - Security and confidentiality.
 - The removal or destruction of individual identifiers at the earliest reasonable time.
 - The prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that public body.

- The person to whom the information is disclosed has signed an agreement to comply with the approved conditions, the FOIPP Act and any of the public body's policies and procedures relating to the confidentiality of personal information.

The provision enables research to take place while at the same time ensuring that privacy is protected. This is accomplished by the strict conditions set out above. For a research project to be considered under this provision *all four requirements must be met*.

For a research purpose means for the purpose of a systematic investigation or study of materials or sources in order to establish facts or to verify theories.

Statistical research is research based on the collection and analysis of numerical data using, in this case, quantifiable personal information to study trends and draw conclusions.

Individually Identifiable Information

Information is in *individually identifiable form* if unique identifiers are attached to the information such that the information clearly pertains to a particular person. The identifiers might be an individual's name, address, telephone number, date of birth, social insurance number or personal health number.

Section 39(a) makes provision for situations where:

- The research purpose cannot reasonably be accomplished unless the information is provided in individually identifiable form; or
- The research purpose has been approved by the Information and Privacy Commissioner.

The first part of this provision allows public bodies to disclose personal information for research in circumstances where the research cannot be completed without access to the information in individually identifiable form.

This might be the case where, for example, there is no intention to use individually identifying information in the research but it would be impractical to sever the personal information because of the volume of the records, the intertwined nature of the personal information or time constraints on the research project.

The second part of the provision allows public bodies to disclose personal information for research if the Information and Privacy Commissioner approved the research purpose.

Approval by the Commissioner ensures that the research purpose is subjected to impartial scrutiny.

In this case, the researcher would submit the proposal to the Commissioner in writing, clearly explaining the nature of the research, the information involved and the reason for the request that he approve the research.

Record Linkage

Section 39(b) places controls on any record linkage performed during a research project.

Record linkage is a form of data matching involving the systematic comparison of sets of information, often personal information, to establish relationships among data. Within the research context, it often involves the creation of a new database allowing the statistical correlation of research variables. Record linkage can be a useful tool for quantitative analysis in research projects.

Record linkage for research purposes is the matching of sets of personal information to achieve the objectives of the research project, with no intention of making decisions about the research subjects' rights or privileges. The matching is a means of linking the right information to the right people in a representative sample used in a study.

This makes it distinct from the kind record linkage for individual *profiling* that is used in some marketing strategies, for example.

Record linkages permitted under section 39 are only for research purposes and no decision that directly affects an individual may be made as a result of such linkage.

The provision also requires that a linkage *not be harmful*. This means that a linkage must not have an adverse affect on the individuals under study – that is, the information disclosed must not result in damage to an individual's reputation, or denial of a job, benefit or service.

Finally, linkages need to be considered in terms of the *benefits derived* from them. The benefits of the research and linkage must override the invasion of privacy that occurs with the disclosure of personal information to the researcher. The research and linkage must be *clearly in the public interest*. That is, the benefits must apply to a wide public and not to just one or two individuals.

Approval of Conditions

Section 39(c) provides that a disclosure for research purposes may take place only if the public body is aware of and has approved the researcher's proposed practices for handling personal information.

Security refers to the physical protection or guarding from unauthorized access or disclosure, theft or other danger of the personal information used in a research project.

Good security may require such measures as locked filing cabinets, computer controls and access codes, restricted work areas, and encryption or encoding of data, depending on the sensitivity of the data involved and the threat and risk associated with it.

Confidentiality means keeping personal information private and safe from unauthorized access, use or disclosure. It means that there is no disclosure, orally or otherwise, other than to those working on the project. For sensitive personal information, disclosure should be on a “need-to-know” basis.

Removal or destruction of individual identifiers means the deletion of identifying information, such as name, address, social insurance number or other numerical identifier, or the destruction of the identifiers in whatever way is appropriate to the medium on which the information is stored. This must be done in such a way as to render the information anonymous.

Removal of identifiers is to take place at *the earliest reasonable time*. This will vary with the circumstances of the case and the comparisons the researcher is making between different sets of data. However, the researcher and the public body should agree on a specific date when a researcher can strip off all identifiers because all the different sets of information have been combined and are ready for analysis.

Prohibition on any subsequent use or disclosure means a prohibition on any further use or disclosure of the personal information by the researcher for any purpose, including any other research or statistical purpose. It can only be used for the project for which the information was originally disclosed, unless the public body explicitly authorizes another research use. This prohibition includes a ban on the use of the information to sell products or services to the subjects of the study and a ban on the sale or gift of the information to a charity in order to help solicit donations.

Agreement to Comply with Approved Conditions

Section 39(d) provides that the researcher must sign a detailed research agreement. This agreement should include the following provisions:

- Personal information disclosed can only be used for a research purpose set out in the agreement or for which written authorization has been given by the public body.
- The names of those persons who will be given access to the personal information must be provided.
- The researcher must bind these persons, through an agreement, to adhere to the same conditions as the researcher.
- Information must be kept in a secure location.

- How and when the identifiers will be removed or destroyed must be specified.
- Contact with the individuals to whom the information relates is prohibited without prior written authority from the public body.
- No use or disclosure can be made of the information in a form that identifies individuals without prior written authorization from the public body.
- Information cannot be used for an administrative purpose directly affecting an individual.
- Notification is required if any conditions of the agreement are breached.
- Failure to meet the conditions may result in cancellation of the agreement and leave the researcher open to charges under **section 75(1)** of the Act.

The Proposal for Access to Personal Information for Research and Statistical Purposes Form and the related Agreement are suitable for an individual or group of researchers that is not part of any public body. If another public body proposes research, a Personal Information Sharing Agreement would likely be more appropriate.

7.11 DISCLOSURE OF INFORMATION IN ARCHIVES

Section 40 provides for the disclosure of information without a FOIPP request by the Public Archives and Records Office or the archives of a public body.

This section is intended to support research by allowing access to archival holdings for research, subject to a limited number of restrictions. Like **section 37**, **section 40** is *enabling*. It *permits* the archives to disclose information *under specified conditions*; it does not *require* the archives to disclose information.

The section does not apply to records that were deposited in the Public Archives and Records Office before the FOIPP Act came into force (**section 3(b)**).

Disclosure of Information by the Public Archives and Records Office or the Archives of a Public Body

The Public Archives and Records Office and the archives of public bodies may disclose information for research purposes subject to certain conditions. The role of the Public Archives and Records Office and other public body archives is to select, preserve and make available the non-current records of public bodies that have been preserved because of their enduring value. This includes legal, evidential, financial, and historical value.

For research purposes means for the purposes of a systematic investigation or study of materials or sources in order to establish facts or to verify theories. *Research* includes general historical and genealogical research.

The *archives of a public body* means an agency, other than the Public Archives and Records Office, that is authorized to perform archival functions on behalf of that public body.

Disclosure of personal information (section 40(a):

This provision supplements **section 37(1)**, which also allows for the disclosure of personal information without a FOIPP request.

If personal information is *less than 25 years old*, archives may not disclose it under **section 40(a)**. The archives must either apply a relevant provision in **section 37(1)** to respond to a request or ask the requester to submit a FOIPP request.

If the personal information requested is 25 or more years old, the archives may disclose the information under **section 40(a)(i)** if:

- The disclosure would not be an unreasonable invasion of privacy under **section 15**;
- The disclosure is in accordance with **section 39**, which specifies conditions for disclosure of personal information for a research purpose; or
- The information is about an individual who has been dead for 25 years or more.

Chapter 4.4 sets out guidelines for applying **section 15**.

If the researcher cannot prove that the individual has been dead for at least 25 years, and it is determined, after application of the other provisions of **section 15**, that the disclosure would be an unreasonable invasion of a third party's privacy, the archives can only disclose the information in accordance with **section 39**, which requires a research agreement.

Information about research agreements and the application of **section 39** is provided in section 7.10 of this chapter.

Archival institutions must not release the personal information of family members or other people who are still living or not dead 25 years along with information about the individual who qualifies for this provision. They must also exercise caution in releasing information about the deceased individual which might be embarrassing or hurtful to family members still living or which may be an invasion of their privacy. Archival institutions must balance the protection of privacy of these individuals against the public interest in the proposed research for which disclosure is considered necessary.

If the personal information is in a record that is *75 or more years old*, the archives may disclose that information. This recognizes that the sensitivity of personal information decreases over time and that disclosure for research purposes is unlikely to result in an unreasonable invasion of anyone's privacy after 75 years.

Nevertheless, archival institutions must remember that this is a discretionary provision and weigh the potential invasion of privacy involved when deciding whether or not to disclose personal information which qualifies for this provision for research purposes.

Disclosure of Information other than Personal Information (section 40(b))

This provision allows for the disclosure of information, other than personal information, which is 25 or more years old. It supplements **section 73**, which allows the heads of public bodies to specify certain categories of information that may be made available to the public without a FOIPP request.

Section 40(b) is intended to establish greater transparency for archives, which tend to hold large volumes of records collected by public bodies. This transparency benefits not only public bodies that transfer the custody and control of their records to archives, but also the researchers who use the collections.

Section 40(b) requires the Public Archives and Records Office or the archives of a public body to assess the information and determine whether disclosure could still result in harm or whether disclosure may be prohibited for some other reason.

Information may be disclosed under this provision if:

- Disclosure would not harm the business interests of a third party within the meaning of **section 14**.
- Disclosure would not harm a law enforcement matter within the meaning of **section 18**.
- The information is not subject to any type of legal privilege under **section 25**.
- Access to the information is not restricted or prohibited by another Act of Prince Edward Island or Canada.

Details on the application of **section 14** are provided in Chapter 4.3 of this publication. If the information is in a record that has been in existence for 50 years or more, then **section 14** does not apply.

Details on the application of **section 18** are provided in Chapter 4.7 of this publication.

Details on the application of **section 25** are provided in Chapter 4.14 of this publication.

When public bodies transfer records to archives, they should identify any records that may be subject to restrictions imposed by other Acts. They should also identify any records to which the exceptions in the FOIPP Act for disclosure harmful to the business interests of a third party or harmful to law enforcement may apply, as well as any records that may be subject to legal privilege.

7.12 EXERCISE OF INDIVIDUAL RIGHTS BY OTHER PERSONS

Section 71 of the Act provides that another individual, under specific circumstances, may exercise any right or power under the Act that is conferred on an individual.

Deceased Individual (section 71(1)(a))

If an individual is deceased, the individual's personal representative can exercise rights and powers under the Act. This exercise of rights and powers is limited to information relating to the administration of the individual's estate.

Proof of the right to act is normally a copy of the signed and attested document naming the representative to act in matters related to the estate.

Evidence consisting of an applicant's stated belief in their authority, whether by affidavit or otherwise, or evidence that an applicant administered an estate is not sufficient.

For information related to disclosure to relatives of deceased persons see Chapter 4.4 and section 7.8 of this chapter.

Guardian or Trustee (section 71(1)(b))

If a guardian or trustee has been appointed for the individual, the exercise of rights can be undertaken by the guardian or trustee. The rights or powers must relate to the powers and duties of the guardian or trustee.

The document governing the nature of the guardianship or trusteeship provides the authority for the representative to act. Public bodies should examine that document to ensure that the disclosure relates to the powers and duties stipulated in the document.

Power of Attorney (section 71(1)(c))

A power of attorney is an authority given to one person (called the attorney) to do certain acts in the name of, and personally representing, the person granting the power (called the donor).

A power of attorney can be to perform specific acts on behalf of the donor (the person who gives the power of attorney) or can be a general power of attorney to do everything that the donor can do. Donors can revoke some powers of attorney; some are irrevocable. Powers of attorney come into effect in the event of mental incapacity or remain in effect notwithstanding the mental incapacity of the donor, provided they comply with the provisions of the *Powers of Attorney Act*. The death of a donor normally revokes the power of attorney.

Public bodies should verify the identity of the person holding the power of attorney and ensure that the power of attorney allows for the disclosure requested or any other power or right being invoked.

It may also be necessary, depending on the nature of the power of attorney, to verify that the donor is alive or that the donor is not suffering from a mental incapacity.

Minors (section 71(1)(d))

If the individual is a minor, a guardian of the minor may exercise any right or power under the Act. This provision does not create an unlimited right of access on the part of a parent or guardian. **Section 71(1)(d)** is discretionary, and disclosure may be limited to circumstances where, in the opinion of the head of the public body concerned, the exercise of the right or power by the guardian would not constitute an unreasonable invasion of the personal privacy of the minor.

The *Age of Majority Act* states that a person ceases to be a minor on attaining the age of eighteen years.

Records should be carefully reviewed in any situation where the information may be sensitive.

A *guardian* is a person who has care and custody of the minor or is involved in their daily care. This definition may not extend to the parents of a child in all circumstances.

Public bodies should have policies for dealing with minors based on the statutes and regulations under which they operate. When seeking decisions from individuals under the age of majority, public bodies should take into consideration their own policies and procedures for deciding when these individuals have the ability to understand the matter being decided and to appreciate the consequences of such a decision. The opinions and views of the minor constitute just one of the factors that must be taken into account in making a decision.

For information on the interpretation of **section 15** and the tests used to determine whether a disclosure would be an unreasonable invasion of privacy, see Chapter 4.4 of this publication.

Proxy (section 71(1)(e))

If an individual has appointed a proxy to make decisions on their behalf, the proxy can exercise the individual's rights. The rights or powers are limited to the powers given to the proxy under the *Consent to Treatment and Health Care Directives Act*. Public bodies should examine the directive before disclosure.

Written Authorization (section 71(1)(f))

Any individual can provide written authorization to another person to act on their behalf. This authorization must be in writing, should generally provide authority to the representative to exercise any right or undertake any power, including the right to provide consent under various provisions of the Act, and be signed by the individual, preferably with an attestation by a witness. The Authorization of Representative Form may be used in this case.

Notices

Section 71(2) provides that any notice required to be given to an individual under the Act may be given to the person entitled to exercise the individual's rights and powers as provided in **section 71(1)**.

CHAPTER 8

Information and Privacy Commissioner

8.1 OVERVIEW

The FOIPP Act establishes an Information and Privacy Commissioner to monitor compliance by public bodies with the provisions of the FOIPP legislation and to investigate complaints. The powers of the Commissioner are set out in **sections 50 to 56** of the Act. The role of the Commissioner in conducting reviews and inquiries is set out in **sections 60 to 68**.

8.2 APPOINTMENT

The Information and Privacy Commissioner is an Officer of the Legislature and is independent of government.

Section 42 of the Act provides that the Legislative Assembly, on the recommendation of the Standing Committee on Legislative Management, appoint the Information and Privacy Commissioner to carry out the duties and functions set out in the Act.

The Commissioner is appointed for a term not to exceed five years and is eligible for reappointment. The Commissioner shall not be a Member of the Legislative Assembly (**section 42**). The Commissioner may resign, but may be removed or suspended from office only for cause or incapacity (**section 44**). This means that the Commissioner may not be removed by arbitrary or capricious action, but only for some reason affecting or concerning the ability or fitness of the Commissioner to perform the duties of the office.

8.3 MANDATE AND POWERS

Part 3 of the FOIPP Act establishes the position of Information and Privacy Commissioner. The Commissioner has a continuing responsibility to ensure that public bodies are complying with the letter and spirit of the Act.

The general powers of the Commissioner are listed in **section 50**. The Commissioner has general responsibility for monitoring how the legislation is administered to ensure that its purposes are achieved. Examples of such monitoring might include:

- Carrying out investigations to ensure compliance with any provision of the Act or compliance with rules relating to the destruction of records. This includes destruction in accordance with rules set out in any other enactment of Prince Edward Island, in a by-law, resolution or any other instrument by which a public body acts, or as authorized by the governing body of a public body.
- Making an order regarding duties imposed by the Act, administrative matters and the collection, correction, use or disclosure of personal information as described in **section 66(3)**, whether or not a review is requested.
- Informing the public about the Act.
- Commenting on the implications for freedom of information or protection of personal privacy of proposed legislative schemes or programs of public bodies.
- Commenting on the implications for protection of personal privacy of using or disclosing personal information for record linkage.
- Authorizing the collection of personal information from sources other than the individual the information is about.
- Bringing to the attention of the head of a public body any failure to assist applicants under **section 8**.
- Giving advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under the Act. The Commissioner may use this power in order to suggest improvement to the way a public body deals with requests. This could be used when there is evidence of poor administration, such as inadequate training or failure to locate records; where there is wanton disregard for the provisions of the Act; or where there are systemic problems, such as regular delays, improper interpretation of exceptions or complaints about breaches of privacy.

Further, without limiting the general powers in **section 50(1)**, the Commissioner may investigate complaints from the public that:

- A duty imposed by **section 8** (duty to assist applicants) has not been performed (**section 50(2)(a)**).
- An extension of time for responding to a request is not in accordance with **section 12** (time extensions) (**section 50(2)(b)**).
- A fee required under the Act is inappropriate (**section 50(2)(c)**).
- A correction of personal information requested under **section 34(1)** has been refused without justification (**section 50(2)(d)**).
- Personal information has been collected, used or disclosed by a public body in violation of **Part 2** of the Act (**section 50(2)(e)**).

An order issued by the Information and Privacy Commissioner is *final* (**section 67**). The Courts have their inherent and constitutional jurisdiction to review and determine whether the Commissioner has acted within the authority given to the Office under the Act. This is known as the principle of *judicial review* and is governed by the *Judicial Review Act*.

As an independent Officer of the Legislature, the Commissioner reports annually to the Speaker of the Legislative Assembly describing the work of the Commissioner's Office, any complaints or reviews resulting from a decision of a public body, and other matters relating to freedom of information and protection of personal privacy (**section 59**).

8.4 MONITORING ROLE

A number, but not all, of the powers of the Commissioner are discussed below.

The Commissioner may investigate the administration of the Act by public bodies. The Commissioner may also audit the practices of public bodies in the areas of freedom of information and protection of privacy.

In the area of freedom of information, the Commissioner may, for example:

- Examine a public body's compliance with the time limits imposed by the Act;
- Review a public body's compliance with the Act requirements for third party notification;
- Investigate allegations that records are being destroyed to avoid producing them in response to a request under the Act;
- Investigate whether a public body is acting appropriately in the disclosure of information in the public interest under **section 30**; or
- Review the decision of the head of a public body to refuse a request for a fee waiver, if requested to do so by the applicant (**section 76(4.1)**).

In the area of privacy protection, the Commissioner may, for example:

- Investigate a public body's disclosures of personal information to third parties to ensure that they are in accordance with the requirements of **section 37** of the Act;
- Review the collection of personal information by a public body to ensure it has the legal authority to collect the information (**section 31**) or is complying with the rules for indirect collection (**section 32**);
- Review the records disposition practices of a public body to ensure that it is retaining personal information as required by **section 33(b)** of the Act; or
- Investigate the application of new information technology to ensure that privacy rights of individuals are being adequately addressed and protected.

The Commissioner's role in dealing with reviews and complaints from persons not satisfied with the handling of a FOIPP request or correction of personal information is discussed in section 8.13 of this chapter.

8.5 PROVISION OF ADVICE

The Commissioner may provide the head of a public body with advice and recommendations on matters respecting the rights or obligations of a head under the Act. Further, the head of a public body may ask the Commissioner to give advice and recommendations on any matter respecting any rights or duties under the Act (**section 51(1)**).

Some examples of advice given under **section 50** have been provided earlier in this chapter. The Commissioner may include advice or recommendations in an order or an investigation report.

The head of a public body might seek advice from the Commissioner on general procedures or matters of interpretation relating to an access request or on how to appropriately apply the privacy protection provisions of **Part 2** of the FOIPP Act. The advice will normally be sought through a letter from the head of a public body to the Information and Privacy Commissioner.

Advice given in response to a request from the head of a public body must be of a general nature and not anticipate or relate to a specific case. It can include recommendations on the administration and application of the Act generally in a particular public body.

Section 51(2) provides that the Commissioner may respond to the head of a public body in writing with advice and recommendations that:

- State the material facts either expressly or by incorporating facts stated by the head.
- Are based on these facts.
- Are based on any other considerations that, in the opinion of the Commissioner, are appropriate.

8.6 DISCLOSURE TO THE COMMISSIONER

As discussed in Chapter 6 of this publication, the Commissioner must investigate and review any disclosure made to them by a public body employee of any information that an employee is required to keep confidential and that the employee, acting in good faith, believes:

- Ought to be disclosed by a head under **section 30** (disclosure in the public interest); or
- Is being collected, used or disclosed in violation of **Part 2** of the Act (**section 69(1) and (2)**).

The Commissioner must not disclose the identity of the employee to any person without the employee's consent.

In carrying out an investigation and review under this provision, the Commissioner has the powers of investigation, mediation and order-making, as well as the protections provided under **Part 4** of the Act (**section 69(7)**).

8.7 POWERS

The Commissioner has all the powers, privileges and immunities of a commissioner under the *Public Inquiries Act* (**section 53(1)**) when conducting a review under **Part 4**, or in giving advice and recommendations under **section 51** of the Act. These include the power to compel witnesses to attend and answer questions at an inquiry and to compel records to be produced.

The Information and Privacy Commissioner of Prince Edward Island, as like the Alberta Information and Privacy Commissioner, is empowered to compel production of information over which solicitor-client privilege is claimed. The Alberta protocol for solicitor-client privilege adjudication has been adopted by our Commissioner. See *Solicitor–Client Adjudication Protocol*, published on the Commissioner's website for guidance on this process.

8.8 ACCESS TO INFORMATION

The Commissioner may require any record to be produced and may examine any information in a record, including personal information, whether or not the record is subject to the provisions of the Act (**section 53(2)**).

A public body must produce any record or copy of a record requested by the Commissioner under **section 53(1)** or **(2)** within 10 days. This must be done regardless of any other enactment of Prince Edward Island but not if a federal enactment, such as the *Young Offenders Act* (Canada), prohibits disclosure. Records must be produced despite any privilege of the law of evidence that might otherwise apply (**section 53(3)**). This requirement applies to records that the public body believes to be excluded from the coverage of the Act under **section 4(1)**.

If a public body is required to produce a record and it is not practicable to make a copy of it, the head of a public body may request that the Commissioner examine the original at the site of the public body (**section 53(4)**).

The Commissioner must return all records or copies of records to the public body after completing a review or investigating a complaint (**section 53(5)**).

8.9 POWER TO DISREGARD REQUESTS

The head of a public body may, under **section 52** of the FOIPP Act, request the Commissioner's authorization to disregard requests from an applicant. This applies to both requests for access to information and requests for correction of personal information. The public body must present facts in support of its request. The Commissioner then makes a decision. The head may be allowed to disregard a request if it is:

- Repetitious or systematic in nature, and
- Processing the request would unreasonably interfere with the operations of the public body, or amount to an abuse of the right to access; or
- Frivolous or vexatious.

A request is *repetitious* if it is one in a series of requests by an applicant for substantially the same information or records.

Requests might be viewed as *repetitious* in cases where an applicant:

- Continues to apply repeatedly for the same or similar information even though the original request has been disposed of and there is nothing new or different in the responsive records;
- Continues to ask for corrections of particular opinions about themselves when a decision has been made and the record has been annotated;
- Makes repeated requests for information which they have been advised is available for purchase; or
- Makes the same request to a public body before a previous request has been completed or any review or investigation procedure carried out.

A request is *systematic* in nature if it is part of an extensive pattern of related requests by an applicant or a group of applicants.

Requests might be considered *systematic* in nature when a single applicant or a group makes a large number of the same or similar requests.

A public body may only request authorization to disregard repetitious or systematic requests if processing the request would *unreasonably interfere with the operations of the public body* or *amount to abuse of the right of access*.

Unreasonable interference with the operations of a public body might be demonstrated by showing the impact that particular repetitious or systematic requests are having on the resources needed to respond within a public body and the actual costs of providing a response.

Abuse of the right of access arises when the action of an applicant is demonstrably a misuse of the FOIPP Act. It may be obvious that requests are not being made to obtain information or achieve a legitimate correction of information, but rather to tie up the resources of the public body or frustrate the administration of a particular program or activity.

A request may be *frivolous or vexatious* if it has no sound basis in fact or is malicious. The applicant may not be making repeat requests or abusing their rights of access under the Act, although that may be the case.

Public bodies might support an argument that a request is frivolous or vexatious with reference to a past pattern of conduct that indicates an abuse of the process for access or with evidence that shows that the request is made in bad faith or for a purpose other than to obtain access to information.

Examples of requests that might be considered frivolous or vexatious include:

- Continual requests for records that a public body has already established it does not have.
- Requests involving fees made by an applicant who has demonstrated a pattern of abandoning a request whenever a fee waiver is not granted or the Commissioner upholds a fee.
- Requests that show an intention to harass a public body, to “break” the system or to engage in “information warfare”.

In one case from another jurisdiction, for example, it was reported that an applicant made a large number of requests to public bodies and had 75 reviews and privacy complaints before the Commissioner’s office.

When requesting the Commissioner’s decision in such a case, the public body might provide evidence of the considerable costs and time involved in dealing with a particular applicant or group of applicants.

No single factor will determine whether a request is frivolous or vexatious. Public bodies need to present a case based on the history of requests by an applicant and the context of those requests when asking for permission to disregard a request.

Asking for authorization to disregard requests should be rare. Public bodies should ensure that they have fully discharged their duty to assist applicants in a full and forthright manner and have a strong case before seeking permission from the Commissioner to disregard requests from one or more applicants.

8.10 STATEMENTS PROVIDED TO THE COMMISSIONER

A statement made or an answer given by a person during an investigation or inquiry by the Commissioner is inadmissible in evidence in court or in any other proceeding, except:

- In a prosecution for perjury in respect of sworn testimony;
- In a prosecution for an offence under the FOIPP Act; or
- In an application for judicial review or an appeal from a decision of that review (**section 54(1)**).

These conditions also apply to evidence from proceedings conducted before the Commissioner (**section 54(2)**).

Anything said, any information supplied or any record produced by a person during an investigation or inquiry by the Commissioner is privileged. The rules that apply are those for a proceeding before a court (**section 55**).

NEW provision added in 2018, s.55.1, that provides that the Information and Privacy Commissioner, and anyone acting for or under their direction, is neither competent nor compellable to give evidence or produce records in a civil proceeding.

Section 56 of the Act places restrictions on the disclosure of information by the Commissioner and the staff of the Office of the Commissioner. They must not disclose any information they obtain in the performance of their duties, with the following exceptions:

- The Commissioner may authorize disclosure of information that is necessary for the conduct of an investigation under the Act or to establish the grounds for findings and recommendations made under the Act (**section 56(2)**).
- The Commissioner may disclose to the Attorney General information relating to the commission of an offence against an enactment of Prince Edward Island or Canada, if the Commissioner believes there is enough evidence of an offence (**section 56(4)**).
- The Commissioner may authorize disclosure of information in the course of a prosecution for perjury or for an offence under the Act, or in an application for judicial review or an appeal arising from that application (**section 56(5)**).

This section allows the Commissioner to request that the police lay charges under **section 75** of the Act.

During the conduct of an investigation, inquiry or audit, the Commissioner and the staff of the Commissioner's Office must not disclose any information that the head of a public body would be required or authorized to withhold from disclosure. They must also ensure that they do not disclose the fact that information exists where, in the notice of refusal to provide access, the public body did not indicate whether or not the information existed (**section 56(3)**).

8.11 PROTECTION FROM LIABILITY

The Commissioner and the staff of the Commissioner's Office are not liable for anything they do in good faith in the exercise of their duties under **Part 3**, Office and Powers of the Information and Privacy Commissioner, and **Part 4**, Review and Complaints, of the Act (**section 57**).

As long as the Commissioner and their staff act honestly and with the intention of complying with the Act, no action can be brought against them.

8.12 DELEGATION OF THE COMMISSIONER'S POWERS

Section 58(1) provides that the Information and Privacy Commissioner may delegate, in writing, to another person any function of the Commissioner under the Act, except:

- The power to delegate under this section.
- The power to examine information described in **section 18** (law enforcement) or **section 20** (Cabinet confidences).
- The power to issue an Order following an inquiry under **section 66**.

8.13 REVIEWS AND INVESTIGATIONS

Reviews

Section 60 of the FOIPP Act provides persons who have made a FOIPP request with the right to ask the Information and Privacy Commissioner to review any decision, act or failure to act by a public body (**section 60(1)**).

Third parties have the right to ask the Commissioner to review the decision of a public body to provide access to records that might harm their personal privacy or business interests.

The public body's decision in response to a request for third party information may be either to grant access to all or part of a record containing this information, or not to grant access. If the public body decides to grant access, the third party may request a review before any records or parts of records are disclosed (**section 60(2)**).

A person who believes that their personal information has been collected, used or disclosed in violation of **Part 2** of the Act may also ask the Commissioner to review the matter (**section 60(3)**).

A relative of a deceased individual may ask the Commissioner to review a decision of a public body under **section 37(1)(aa)** not to disclose personal information about the deceased individual (**section 60(4)**).

The right to an impartial review of decisions or actions of a public body is fundamental to guaranteeing freedom of information and protection of privacy rights. The review mechanism ensures that these rights are interpreted consistently among public bodies and the purposes of the Act are achieved. The orders, which summarize the reviews, issues, reasons, and findings of the Commissioner, also provide guidance to public bodies regarding the proper interpretation of the Act.

A review by the Commissioner of the decision of a public body is intended to be an avenue of last resort. In most cases, a person will be satisfied that the public body has acted responsibly and any outstanding issues can be settled between the public body and the person concerned. Even in cases where the person asks the Commissioner to review a decision, issues can often be settled through mediation and an inquiry may not be necessary.

Certain matters that may be the subject of a request for review can also be grounds for a complaint to the Commissioner under **section 50(2)** of the Act.

These are:

- Matters relating to the public body's duty to assist the applicant (**section 8**).
- A decision to extend the time limit under **section 12** for responding to a request.
- The amount of a fee charged or the refusal to waive all or part of a fee under **section 76**.
- A refusal to make a correction to personal information as requested under **section 34(1)**.
- The collection, use or disclosure of personal information in violation of **Part 2** of the Act.

Requesting a Review

Section 61 of the Act sets out the process for requesting a review. Applications for a review must be *in writing*. **Section 71** establishes classes of individuals who may act for deceased persons, incompetent persons, minors and any other individuals in exercising this right under the Act.

A person must deliver a request for a review to the Commissioner within 60 days of receiving notification of a public body's decision or a longer time when allowed by the Commissioner (**sub-section 61(2)(a)**). Third parties have only 20 days in which to seek a review (**sub-section 61(2)(b)**).

Failure by a public body to respond in time to a request for access to a record is treated as a decision to refuse access (deemed refusal). In this case, there is no notification by the public body.

Preparation for a Review

A public body must be able to show that it has properly fulfilled its duties under the Act. It should document the reasons for each decision relating to the withholding of records or parts of records and should ensure that the circumstances surrounding the request support each action it takes.

To reduce the need for review of decisions, public bodies should provide applicants and third parties with clear explanations of their decisions, the provision(s) of the Act that apply and the reasons why they are applicable in the particular instance. These explanations provide a basis for discussion of the decision and may help the public body and the person to settle any outstanding issues without recourse to the Information and Privacy Commissioner. If a particular case for review deals with an issue that has implications across government or affects most public bodies, the public body should consult with the Access and Privacy Services Office in the Office of the Attorney General.

Review Process

The Information and Privacy Commissioner develops the procedures for conducting a review. The Act has enabling provisions and some requirements governing the review process.

Upon receiving a request for review, the Commissioner must provide a copy of the request to the head of a public body and to any other person the Commissioner deems appropriate (**section 62(1)**).

The Commissioner may sever any information in the request that is considered appropriate before providing copies as stated above (**section 62(2)**). This is necessary because applicants may include personal information as a part of their requests for review, and it may not be appropriate to disclose this to the public body or other persons.

The Commissioner, the public body and the applicant may jointly review the request to determine whether or not the concerns raised in it can be addressed through mediation.

The Commissioner will also likely ask the public body to submit copies of the following documentation, where applicable:

- The FOIPP request.
- Notice of the public body's decision.
- Any correspondence related to the request, issue or decision.
- An index of the relevant records and exceptions relied upon.
- Severed and unsevered copies of the records; and, where applicable.
- Descriptions of personal information in the public body's personal information banks and policies and procedures for its management under **Part 2** of the Act.

The public body will initially be more familiar with the issues involved than the Office of the Commissioner. If the public body has any information concerning affected persons who should be notified of the review, it should inform the Commissioner's Office as soon as possible.

It should also make known any relevant issues, considerations or factors that affected the making of the particular decision. The Commissioner will have a better understanding of the public body's position if it can demonstrate that it made every effort to meet a person's needs and to resolve outstanding issues.

Mediation

Section 63 provides that the Commissioner may authorize a mediator to investigate and try to settle any matter that is the subject of a request for a review. The mediator does not impose a settlement. Rather, mediation is intended to help the public body and the person requesting a review to arrive at a settlement before a formal inquiry is initiated.

Inquiry

If a mediator is not appointed or the matter is not resolved with the help of a mediator, the Commissioner normally conducts an inquiry (**section 64**). In the course of the inquiry, the Commissioner will decide all questions of law and fact. The Commissioner's powers in conducting inquiries are provided in **sections 53** and **64** of the Act.

The Commissioner has broad discretion to determine how an inquiry will be conducted. It may be conducted in private (**section 64(2)**) and the Commissioner may decide whether representations are to be made orally or in writing (**section 64(4)**).

The person who asked for the review, representatives of the public body concerned and any person given a copy of the request for review are entitled to make representations to the Commissioner during the inquiry (**section 64(3)**). They may choose to be represented by counsel or an agent (**section 64(5)**).

No party has a right to be present during another party's representations, to have access to or to comment on representations made by another person during the inquiry process (**section 64(3)**).

In the case of a refusal of access, the Commissioner has the right and duty to view all records that have been withheld from disclosure in whole or in part. This right pertains regardless of the exception that the public body has used or the fact that the public body believes the records are excluded from the scope of the Act.

The Commissioner may require the records to be produced within 10 days (**section 53(3)**). The Commissioner must return such records to the public body upon completion of the review (**section 53(5)**).

The head of a public body may require the Commissioner to examine a record at the site at which it is being held, if it is not practical to make a copy (**section 53(4)**). This could occur, for example, when a record is too fragile to copy or the copying process would damage the record. Public bodies should avoid, as much as possible, requiring on-site examination of records since it will place an additional administrative burden on their own and the Commissioner's operations.

The Commissioner may compel witnesses to attend an inquiry and answer questions. The Commissioner has all the powers of a Commissioner provided under the *Public Inquiries Act*. These include the power to compel attendance at an inquiry and to compel records to be produced.

Refusal to Conduct Inquiry

Over time, issues raised in requests for review may replicate issues already dealt with by the Commissioner. If the Commissioner believes that the subject matter of a request has already been dealt with in an order or an investigation report, the Commissioner may refuse to conduct an inquiry (**section 64.1**).

Time Limits for Review

Normally, the Commissioner's inquiry must be completed within 90 days after receipt of the request for review (**section 64(6)**). This time limit encompasses all elements of the review process, including mediation and any formal inquiry.

However, the Commissioner may notify all parties to a review that they are extending the period for the review and establish a date for the completion of the review (**section 64(6)**). The intent of the Act is to ensure that an independent review of decisions can take place, so even if the process is not completed within the extended time limit, the Commissioner has the power to complete the inquiry.

Burden of Proof

Section 65 establishes where the burden of proof lies in various situations relating to access to records. Normally, the burden of proof rests with the public body refusing access to all or part of a record (**section 65(1)**), unless the request is for a record or part of a record that contains personal information about a third party.

This means that under normal circumstances the public body must prove, on the balance of probabilities, that particular information may be excepted from release under the Act or excluded from its scope.

Careful documentation of the reasons for refusing the request will form the central arguments that will meet the burden of proof.

A public body also has the burden of proof in cases where an applicant has requested a review of fees charged. This is because the public body has all the information about the assessment and calculation of fees.

When a public body has refused to disclose personal information under **section 15**, which requires public bodies not to disclose personal information if the disclosure would be an unreasonable invasion of an individual's privacy, the burden of proof rests with the party requesting disclosure of the personal information.

The applicant requesting the personal information must show that disclosure would not be an unreasonable invasion of the personal privacy of the individual to whom the information relates (**section 65(2)**).

When a third party has requested a review of a public body's decision to disclose a record or part of a record containing personal information about the third party, the burden of proof also lies with the applicant who has requested disclosure of the personal information.

The applicant must show that disclosure will not constitute an unreasonable invasion of the privacy of the individual the information is about (**section 65(3)(a)**).

When the inquiry concerns a public body's decision to disclose third party business information (**section 14**), the burden of proof lies with the third party resisting disclosure. That is, the third party must demonstrate that the applicant has no right of access to the record (**section 65(3)(b)**).

Commissioner's Orders

Upon completion of an inquiry, **section 66** of the Act requires the Commissioner to make an order. If the inquiry concerns a refusal to grant access to all or part of a record, the Commissioner must order one of the following:

- Require the public body to give access to all or part of the record;
- Confirm the decision of the public body or require the head to reconsider a decision to refuse disclosure; or
- Require the head to refuse access to part or all of the record requested.

When the Commissioner finds that a refusal to grant access is in compliance with the Act, and the head has properly exercised their discretion, the Commissioner may only confirm the decision of the public body or request that the head reconsider the decision based on their exercise of discretion.

The Commissioner can only require the head of a public body to reconsider a decision to *refuse* access, not a decision to *grant* access.

If the inquiry concerns any other matter, such as the matters discussed in **section 5(2)**, the Commissioner may make an order requiring compliance with the provisions of the Act.

Section 66(4) provides that the Commissioner may attach any terms or conditions to an order. A copy of the order is given to the person who asked for the review, the head of the public body concerned, any person given notice of the review under **section 62** of the Act, and the Minister responsible for the administration of the Act (**section 66(5)**).

The head of a public body that has received an order from the Commissioner must comply with the order no earlier than 30 days after the order, and no later than 40 days after the order (**section 68(1) and (1.1)**). This is to allow an applicant, a third party or the public body time to apply for judicial review.

If an application for judicial review is made, the Commissioner's order is stayed until the Court has dealt with the application (**section 68(2)**).

There is no appeal from an order made by the Commissioner (**section 67**), except a limited appeal through judicial review (see **section 8.13** of this chapter).

It is an offence to fail to comply with an order made by the Commissioner under **section 66**. The Commissioner may choose to file a copy of an order with the registrar of the Supreme Court of Prince Edward Island and, after filing, the order is enforceable as a judgment or order of that Court (**section 66(6)**).

Investigations

Section 50(1) of the FOIPP Act enables the Commissioner to monitor compliance with the Act and carry out investigations into how the Act is being administered to ensure that its purposes are achieved. **Section 50(2)**, without limiting these more general powers, enables the Commissioner to investigate and attempt to resolve complaints that:

- A duty imposed by **section 8** (duty to assist) has not been performed.
- An extension of time for responding to a request is not in accordance with **section 12**.
- A fee under the Act is not appropriate.
- A correction of personal information requested under **section 34(1)** has been refused without justification.
- Personal information has been collected, used or disclosed by a public body in violation of **Part 2** of the Act.

The main difference between an investigation and a review is that an investigation may not be a result of a FOIPP request. A complaint that does not arise from a FOIPP request is most likely to occur in cases involving disclosure in the public interest or allegations of improper collection, use or disclosure of personal information.

Time Limits on Complaints

When an investigation arises from a FOIPP request, the applicant must deliver the complaint to the Commissioner within 60 days of receiving notification of the public body's decision (**section 61(2)(a)**). A longer time may be allowed by the Commissioner (**section 61(2)(b)**). When allowing a delay, the Commissioner will consider all relevant circumstances.

The Act does not specify a time limit for privacy complaints, since these do not, for the most part, arise from a FOIPP request. They tend to stem from a complainant's belief that there has been improper collection, use or disclosure of personal information.

Privacy Investigations and Audits

The Commissioner can take an active role in investigating compliance with Part 2 of the Act. An investigation can be undertaken as a result of a complaint that personal information is not being collected, used, disclosed or protected in accordance with the provisions of the FOIPP legislation.

As well, the Commissioner may decide to conduct an audit of privacy protection in a program of a public body that has custody or control of sensitive personal information.

8.14 ADJUDICATOR PROCESS

Section 68.1 provides for the designation of an adjudicator. The Lieutenant Governor in Council may designate an adjudicator in situations where the Commissioner is not in a position to conduct a review because they have a conflict in relation to the subject matter of the review. For example, the Commissioner may have a conflict if the Commissioner has been a member or employee of the public body that is the subject of the review. The designation of an adjudicator may also occur when the matter under review relates to the Commissioner's Office to any other legislative office of which the Commissioner is appointed Officer.

The determination that the Information and Privacy Commissioner has a conflict of interest is made by the Commissioner. The Commissioner is in the best position to decide whether their decision on a particular matter might later be the subject of a judicial review by the Court on the grounds that the Commissioner had a conflict of interest (a reasonable apprehension of bias).

An applicant or third party seeking a review under these circumstances may request, under **section 68.5(1)** of the Act, that an adjudicator be appointed to conduct a review.

The request for designation of an adjudicator must be in writing and made to the Minister responsible for the FOIPP Act. The request must be made within 60 days of the person receiving notice of the decision to be reviewed, or 20 days if a third party is challenging disclosure of information. The adjudicator may decide that a longer period should be allowed.

A submission is made to Cabinet to authorize the Lieutenant Governor in Council to designate the judge to act as an adjudicator. The minister must provide a copy of the applicant's request for review, together with a summary of the review procedures that will govern the process, to the adjudicator, the Information and Privacy Commissioner and any other person affected by the request.

An adjudicator has the same powers and duties as the Commissioner and can dispose of a matter in the same way. An adjudicator cannot review an Order of the Information and Privacy Commissioner (**section 68.1.(2)**). A copy of the adjudicator's order must be given to the Commissioner. An Order made by an adjudicator is final (**section 68.7(6)**). Adjudication Orders will be made available on the Commissioner's website at <http://www.oipc.pe.ca>

Note that the Commissioner may, under **section 58**, delegate one of their portfolio officers to act as an adjudicator in the office. This officer may be delegated to conduct inquiries and issue Orders. The purpose of this delegation is to distribute the Commissioner's workload in the area of inquiries, not to deal with specific issue of conflict of interest on the part of the Commissioner. The name of "adjudicator" that may be chosen for the delegate is simply an assigned title. It should not be confused with an adjudicator that has been designated by the Lieutenant Governor in Council for the purpose of **section 68.1**.

8.15 JUDICIAL REVIEW

The Information and Privacy Commissioner has exclusive jurisdiction to conduct a review and investigate complaints against a public body under the FOIPP Act. Courts do not have the power to issue orders under the Act.

However, a person may apply to the Supreme Court of Prince Edward Island to exercise its inherent jurisdiction to review any action or failure to act on the part of the Information or Privacy Commissioner. It may also review the decisions of the Commissioner for an error of law on the face of the record, jurisdictional error or breach of natural justice (fairness).

The process for judicial review is governed by the *Judicial Review Act*. Application for judicial review of a decision of the Commissioner must be made not later than 40 days after the party applying for judicial review is given a copy of the decision.

The Court has the power to compel the Commissioner to do something or to refrain from doing something and the power to send a matter back to the Commissioner for reconsideration.

A judicial review is not an appeal of the Commissioner's decision. The Court cannot substitute its own decision for that of the Commissioner. The Commissioner is the final arbiter of questions of fact but is always subject to the overriding jurisdiction of the Court to ensure that the Commissioner acts within their authority.

FOI Request 30-Day Process Chart

Time Lines (Calendar Days)	Key Tasks	Manual References	FOI Tips
Day of Receipt	<ul style="list-style-type: none"> Request received by FOI Analyst. Decision: Routine access to information or FOI request. 	1.9/1.10 Routine disclosure and active dissemination of information 3.2 Receiving a FOI request Duty to assist applicant Clarifying requests	<ul style="list-style-type: none"> The Act does not replace existing procedures for access to information. Provide information through routine channels if possible.
30 calendar days to respond	Thirty-day clock starts		
Day 1 - first working day after receipt <div style="border: 1px solid black; border-radius: 10px; padding: 5px; width: fit-content; margin: 10px auto;"> Clock does not start until initial fee is paid. </div>	<ul style="list-style-type: none"> Request for access to general records or for the applicant's own personal information? If general access request – initial fee paid? Clarify request with applicant. Decide whether request should be transferred. Send acknowledgement to applicant. Notify applicant if request transferred 	1.6 Custody or control 3.2 Receiving a FOI request Form of the request Acknowledging receipt Clarifying requests Transferring a request	<ul style="list-style-type: none"> Clarify with applicant what records/info is wanted. Read the Act section 7(2). It requires a request to be in writing, and provide enough detail to enable a public body to identify records Always be helpful and keep applicant informed. Do not probe motives. Send letter to applicant if initial fee was not received for a general access request. Consult with other public body before transfer.

Time Lines (Calendar Days)	Key Tasks	Manual References	FOI Tips
Day 2	<ul style="list-style-type: none"> Set up request file. Ask program areas to search for records. 	<p>3.2 Receiving a FOI request Documenting and tracking requests</p> <p>3.3 Processing a FOI request – Search and retrieval Locating, retrieving and copying records</p>	<ul style="list-style-type: none"> Information about applicant is only shared on “need to know” basis. Ensure all program areas that may have records are asked to search. Reasonable Search is the right person searching in the right places and spending the right amount time.
Days 2 - 7	<ul style="list-style-type: none"> Program areas retrieve records and forwards with completed record search forms to FOI Analyst. Consider need for time extension if extensive records to be searched. 	<p>3.2 Response time limits Time limit extensions</p> <p>3.3 Processing a FOI request – Search and retrieval Locating, retrieving and copying records</p>	<ul style="list-style-type: none"> Keep accurate and complete documentation of search using Record Search form.
Days 7 – 10	<ul style="list-style-type: none"> Consider fees and send estimate if applicable. Consider need for consultations with public bodies or third parties. Follow up as needed. Consider creation of a record. <div style="border: 1px solid black; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p>If fee estimate is sent to applicant, clock stops until deposit is received.</p> </div>	<p>3.2 Receiving a FOI request Consultation</p> <p>3.3 Processing a FOI request – Search and retrieval Preliminary assessment Assessing fees</p> <p>3.4 Processing a FOI request – Reviewing and preparing records for disclosure</p> <p>3.3 Creating a new record</p> <p>5.2 Third Party Notice</p>	<ul style="list-style-type: none"> Determine whether all relevant records have been located. Stop processing until deposit is received. Consider fee waiver and/or narrowing request. Executive Council must be consulted regarding Cabinet confidences. (See information on section 20 of the Manual.)

Time Lines (Calendar Days)	Key Tasks	Manual References	FOI Tips
End of Day 10	<ul style="list-style-type: none"> Consider whether time extension is needed to complete consultations. Preliminary assessment complete, consultations in process. 	3.2 Receiving a FOI request Consultation 5.9 Response time limits Time limit extensions	<ul style="list-style-type: none"> Public body has 10 days to make decision regarding disclosure of records following reviews with third parties.
Days 10 – 17	<ul style="list-style-type: none"> Detailed line-by-line review. Consider feedback during consultations. Apply exceptions and exclusions. 	3.3 Processing a FOI request- Reviewing and preparing records for disclosure Line-by-line review of records Severing information 4. Exceptions to the Right of Access	<ul style="list-style-type: none"> Continue consultation with program areas. Keep accurate and complete record of reasons for each exception. Keep accurate records of time spent severing records if fee estimate was issued. See "2-minute rule" referenced OIPC Order No. 03-001. Notify applicant, read the Act section 13(1).
Day 15	<ul style="list-style-type: none"> Last day for transferring request. 	3.2 Receiving a FOIP request Transferring a request	<ul style="list-style-type: none"> Consider whether time extension is needed to deal with outstanding external consultations.
Day 17 – 21	<ul style="list-style-type: none"> Consider feedback received via consultations. Apply exceptions and exclusions. 	3.2 Response time limits Time limit extensions 3.3 Processing a FOI request – Reviewing and preparing records for disclosure 4. Exceptions to the Right of Access	
End of Day 23	<ul style="list-style-type: none"> Complete consultations. 		

Time Lines (Calendar Days)	Key Tasks	Manual References	FOI Tips
End of Day 25	<ul style="list-style-type: none"> Send recommendations, and severed records to Head for approval. 		<ul style="list-style-type: none"> Notify Head of sensitive information or issues in records. Once the decision is made, third party has 20 days to ask for review.
Days 25 – 27	<ul style="list-style-type: none"> Act on Heads decision. 	3.3 Processing a FOI request – Reviewing and preparing records for disclosure Severing information	
Day 27 <div>Clock stops until balance of fee received</div>	<ul style="list-style-type: none"> Calculate fees owing and collect from applicant. 	3.3 Assessing fees	
Day 30, or next working day if Day 30 falls on weekend or holiday.	<ul style="list-style-type: none"> Disclose records and decision to Applicant. 	3.4 Responding to an applicant Completion of request and closure of request file	
	<ul style="list-style-type: none"> Close file. 		<ul style="list-style-type: none"> Store file securely and retain according to Records Retention Schedule

FOI FILE #:

RECORD SEARCH FORM

The person who performs the search for records should be the person to complete this form.

Return completed form to APSO 1st Floor, Sullivan Bldg. 902.569.7590

1. Choose one:

- ☐ I have no concerns with these records being disclosed.
- ☐ I have concerns with these records being disclosed.
- ☐ No records found.

2. Describe your concerns related to disclosure of these records. Be specific.

3. **DO YOU HAVE LEGAL CONCERNS WITH THESE RECORDS OR MAY THEY BE SUBJECT TO LEGAL PRIVILEGE?**

☐ Yes ☐ No

IF YES, do not return the records to APSO. Call Bobbi-Jo Dow Baker, APSO Solicitor at 902.218.5614 as soon as possible to discuss.

4. Start date of the search:

5. End date of search:

6. Time (in minutes) to complete search (do not include time spent photocopying records):

7. Provide details about specific areas searched:

Email:	In-box:
Sent box:	Archive:
Other:	Text Messages:
Shared directory:	
Electronic files (provide key words searched):	
Other (provide details):	
File cabinets (provide location / CPRS series headings if possible):	
Records Centre (Consult your RIM Officer)	
Completed by:	Date:

Locating and Retrieving FOI Records

- **A public body must make a reasonable effort** to identify and locate records responsive to a FOI request.
- **A reasonable effort must be adequate, not perfect.** This means the right person spending the right amount of time and looking in the right place(s).
- **A person searching for records should only look for records that are responsive to the request.** If you do not know what you are looking for – immediately seek clarification.
- **An adequate search must consider all records**, including electronic records that are in the custody or under the control of the public body.
 - This may include searching file cabinets located on and off-site (Records Centre), employee computers, and emails, any location where records might be found.
 - Laptops, BlackBerry Phones, or Cell Phones may need to be searched as well.
 - A public body may also have to search for responsive records under its control that are in the hands of a third party. This would include records in the possession of a contractor. A public body is not required to search for records in the custody or under the control of other public bodies.
- **Records and information management staff** may be able to assist in the search.

Completing the Record Search Form

- A public body **must be prepared to support claims that they performed an adequate search.** Completing the Record Search Form in detail is evidence of an adequate search.
- The Record Search Form should be completed and returned even when no responsive records are located.

Legal Privilege

- **If privileged records are located in the search, call Bobbi-Jo Dow Baker, APSO Solicitor at 902.218.5614 to discuss next steps.**



Search in Outlook (The desktop version)



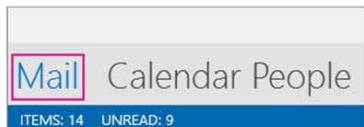
CONTENTS

A. Find a message or item with Instance Search in outlook.....	3
B. Narrow the Search results:.....	5
C. Use Advanced Find	7
D. Remove the Limit of the number of the search result:	10
E. Narrow down your Search criteria:	10
I. Search basics	10
II. Use Outlook's built-in search filters	11
F. Use Search Folders to find messages or other Outlook items.....	11
I. Create and use predefined Search Folders	12
II. Create a customized Search Folder	12
Delete a Search Folder	14
Appendix A: Search Reference Tables	16
Appendix B: Useful Training links (videos and additional training materials).....	21

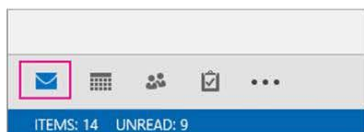


A. FIND A MESSAGE OR ITEM WITH INSTANCE SEARCH IN OUTLOOK

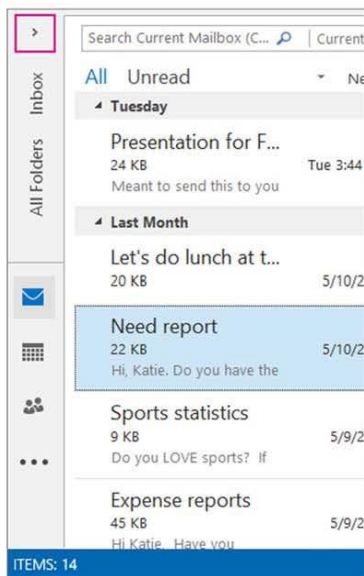
1. In the navigation bar, near the bottom of the screen, click **Mail**.



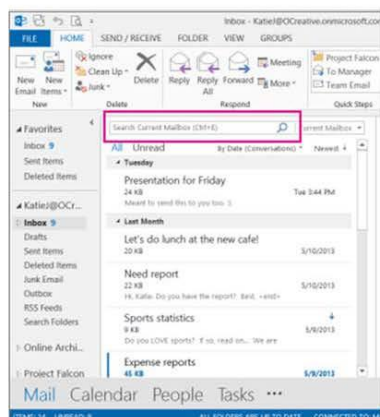
If you don't see this, "Compact Navigation" might be turned on, so you'll see icons instead, like this:



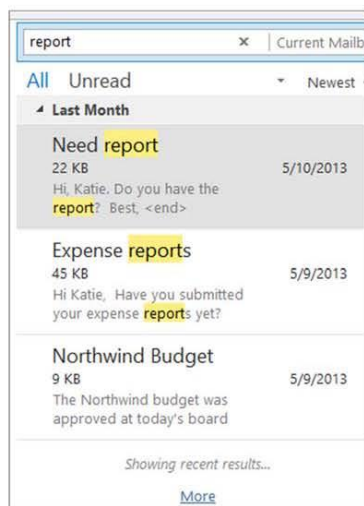
Or, in addition to "Compact Navigation" being on, the folder pane might be minimized, so the icons are arranged vertically. You can expand the folder pane by clicking the **Minimize/Expand** button, as shown here:



2. Find the search box. It's at the top of your messages, as shown here:




3. To find a word that you know is in a message, or a message from a particular person, type the word or person's name (you can use first, last, and partial names) in the search box. Messages that contain the word or name you specified appear with the search text highlighted in the results.



4. You can narrow your results even further by changing your search. Here are some common examples:
 - Type **"expense reports"** (including the quotes) to find messages containing the exact phrase "expense reports."
 - Type **expense AND report** ("AND" needs to be in all caps) to find messages containing both the word expense and the word report, but not necessarily in that order. You can also use "OR."

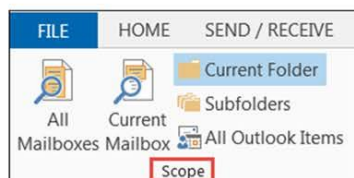


- Type **expense NOT report** ("NOT" needs to be in all caps) to find messages containing the word expense but not the word report.
5. NOTE: Searching will only find items if you search for an entire word, or the beginning of a word; if you search for the middle or end of a word you will not find the item. For example, if the message subject contains "Email about Office365", the following searches will NOT find that item:
- "mail" -- because this is the end of the word "email"
 - "365" -- because this is the end of the word "Office365"
 - "ice" -- because this is in the middle of the word "Office365"
6. When you're finished, you can clear the search by clicking the  in the search box.

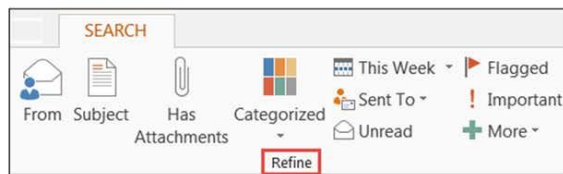
B. NARROW THE SEARCH RESULTS:

If you can't find what you're looking for, use the search tools on the ribbon to narrow down your search. When you click the search box, you can select a scope option on the left side of the ribbon. Once you decide your scope, you can then refine your search further by selecting an option such as the subject line or the sender.

Scope (where to search): Here you can choose to search in specific folders, such as all your mailboxes, or just the current folder you've selected, which is your **Inbox** most of the time.



Refine (what to search for): When you've selected your scope, you can add other criteria in the **Refine** group. When you select an option, Outlook adds a special script to the search box to limit its search.



Let's take a look at the options.



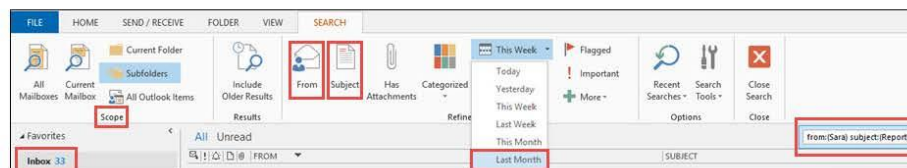
- **From:** filters your search results to only show messages sent by a specific person. For example, you can search for all the messages sent by Sara.
- **Subject:** filters your search results based on the subject line of the email. For example, you can search for all the messages that have the keyword "report" in the subject line.
- **Has Attachments:** gives you all the messages that contain an attachment.
- **Categorized:** choose a category to see all the messages that you've flagged with a specific category.
- **This Week:** on the drop-down menu, choose a time frame to narrow your search results based on the time you received a message.
- **Sent To:** on the drop-down menu, choose an option to filter the results based on the email recipients. For example the messages that you were CCed on, or the ones that were sent to a specific person.
- **Unread:** brings up all the unread messages in the folder that you've selected.
- **Flagged:** brings up messages that you flagged to follow up.
- **Important:** shows all the messages that were marked with high importance.
- **More:** choose an option on the menu to further narrow down your search results. For example you can filter by sensitivity or message size.

Remember that you can mix and match these options.

Here's an example: You can search for all the messages from Sara that you received last month, with the keyword "report" in the subject line.

To set up a search for this example:

1. Make sure **Inbox** is selected, then click in the **Search** box.
2. Select **Subfolders** in the **Scope** group.
3. Click **From** and type *Sara* to replace the highlighted text in the search box.
4. Click **Subject** and type *report* to replace the highlighted text in the search box.
5. From the drop-down menu next to **This Week**, select **Last Month**.

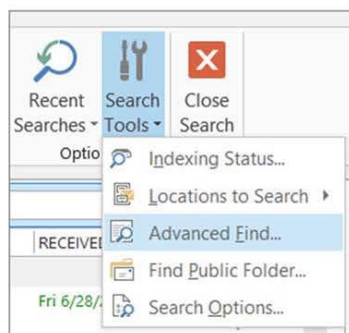




C. USE ADVANCED FIND

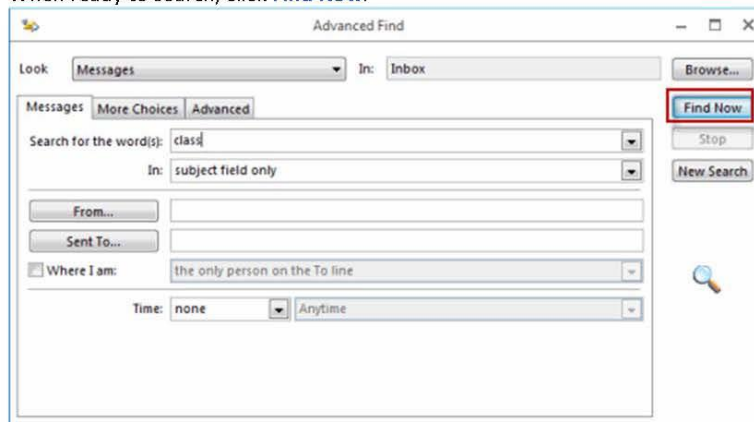
Getting too many results? Or are you just not finding what you want?

1. Click in the search box.
2. On the **Search** tab, click **Search Tools > Advanced Find**.



In the Advanced Find dialog box, configure options such as word to search, time frame, sent to or from, and so on.

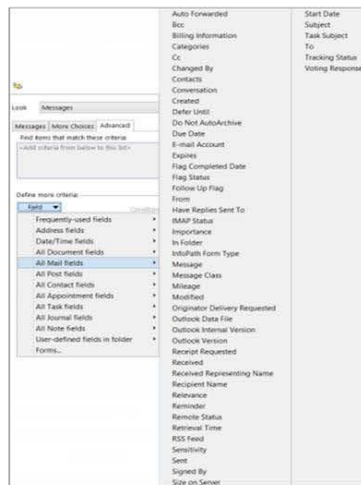
When ready to search, click **Find Now**.





In the **Advanced Find** box, you can specify much more complex criteria and even search in your calendar, contacts list, notes, and tasks.

1. Click the **Advanced** tab.
2. Under **Define more criteria**, click the **Field** button and then click **All Mail Fields**. You'll see a menu of fields you can search on, such as **From**, **To**, **Received**, **Subject**, and dozens more.



3. Start by choosing a field, then choose a condition and a value to test. For example:

From/ Contains/ Katie will search for messages from someone whose name includes "Katie." Notice we're using **contains** as the condition instead of **is (exactly)** so that we don't have to find an exact match. So if Katie's email name is "Katie Jordan," **From/is (exactly)/Katie** won't work because we'd need to specify Katie's full name, Katie Jordan, to get an exact match. That's where **contains** comes in handy as a condition.

4. Add as many additional conditions as you need or want to test. We'll add three more:

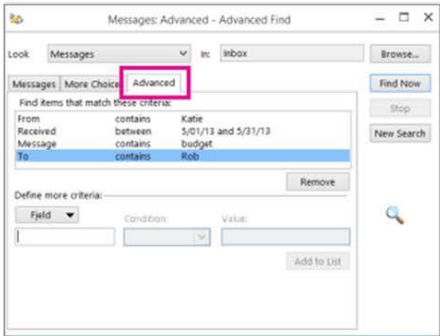
From | Contains | Katie will search for messages from someone whose name includes "Katie." Notice we're using **contains** as the condition instead of **is (exactly)** so that we don't have to find an exact match. So if Katie's email name is "Katie Jordan," **From | is (exactly) |Katie** won't work because we'd need to specify Katie's full name, Katie Jordan, to get an exact match. That's where **contains** comes in handy as a condition.

Then, let's say you add these as well:

- **Received | between | 5/01/21 and 5/31/21**



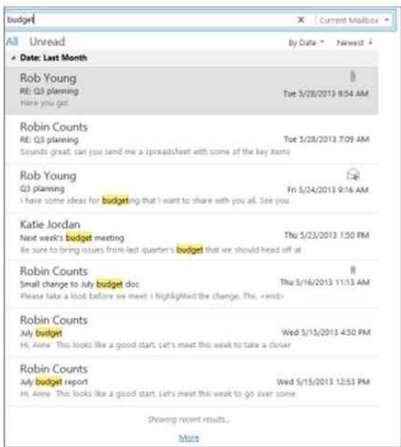
- **Message | contains | budget**
- **To | contains | Rob**



Now, Outlook searches for messages from someone with "Katie" in her name that arrived in the inbox in May, 2013, with "budget" in the message body, and (in addition to you) were also sent to someone with "Rob" in his name. Here's a zoomed look at the list of the four criteria we added.

Find items that match these criteria:		
From	contains	Katie
Received	between	5/01/13 and 5/31/13
Message	contains	budget
To	contains	Rob

Finally, click **Find Now** to run the search.





D. REMOVE THE LIMIT OF THE NUMBER OF THE SEARCH RESULT:

If the thought of more than 250 results doesn't scare you off, you can bypass that limit:

1. Click **File > Options > Search**.
2. Under **Results**, clear the **Improve search speed by limiting the number of results shown** check box.

E. NARROW DOWN YOUR SEARCH CRITERIA:

You can type a number of phrases in the Search box at the top of the Outlook message list. In addition to searching for different words and phrases, you can use various operators, punctuation and keywords to narrow your search results.

The most basic way to search is to simply type in a word or phrase.

NOTE: Outlook uses what's called prefix matching when searching. So if you type **ray** into the Search box, Outlook will return messages that contain *ray*, *Ray*, *Raymond*, and *rays*, but not *disarray* or *tray*. Also, the search treats numbers that are connected to words (no spaces between the word and the number) as part of the word. Searching for "365" will NOT find messages that contain "Office365".

SEARCH BASICS

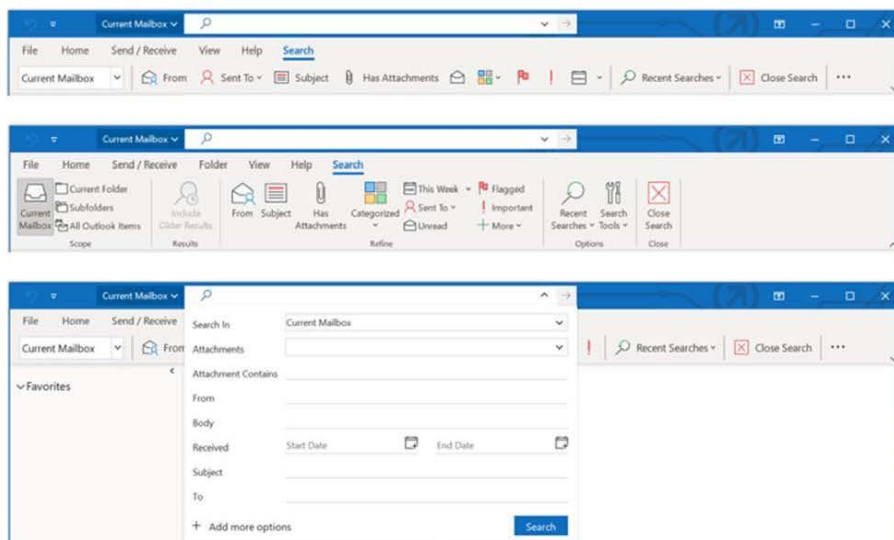
- When you type words into the Search box, Outlook scans both email messages and many types of attachments for that word or phrase. For example, if you search for "project" either with or without quotes, Outlook will return all messages with the word project, projects, projector, projecting, etc. anywhere in the sender name, subject, message body, or attachments.
- When you type in an email address, for example `cheryl.parsons64@yahoo.com`, Outlook returns all email messages that contain that email address anywhere in the subject, message body, or many types of attachments as well as messages from that email address. To limit your search results to emails from an email address, type `from:cheryl.parsons64@yahoo.com` in the search box.



II USE OUTLOOK'S BUILT-IN SEARCH FILTERS

Outlook provides you with a number of built-in search filters. To use the built-in filters, click in the Search box. Based on your preference, you can use Advanced Search by clicking the filter button on the right side of the search box. Alternatively, the Outlook ribbon will change to show the Search tab and you use any of the options in the Refine group to refine your search results.

You can find the search box at the top of the screen whether you are using the Simplified Ribbon or the Classic Ribbon.



F. USE SEARCH FOLDERS TO FIND MESSAGES OR OTHER OUTLOOK ITEMS

A Search Folder is a virtual folder that provides a view of all email items that match specific search criteria. For example, the **Unread Mail** Search Folder enables you to view all unread messages in one folder, even though the messages might be saved in different folders across your mailbox..

Create a new Search Folder: You can create two different types of search folders.

- I. Create and use predefined Search Folders.
- II. Create A customized Search Folder



I CREATE AND USE PREDEFINED SEARCH FOLDERS

1. Select the **Folder** menu.
2. In the **New** group, select **New Search Folder**.

Keyboard shortcut To create a new Search Folder, click Ctrl+Shift+P.

3. From the **Select a Search Folder** list, click the Search Folder you want to add. Some of the predefined Search Folders are only available if you scroll down to the end of the list.
4. If the predefined Search Folder has customization options, you'll see those options appear under **Customize Search Folder**. For example, if you select **Mail with specific words**, under **Customize Search Folder**, specify the words to use.

Note: Search Folders use prefix matching searches when you type specific words to include in the search. For example, if you type "rain" in the word list, the Search Folder will include messages that contain the word "rain" and the word "rainy." The Search Folder will not contain messages that include the words "brain" or "grain."

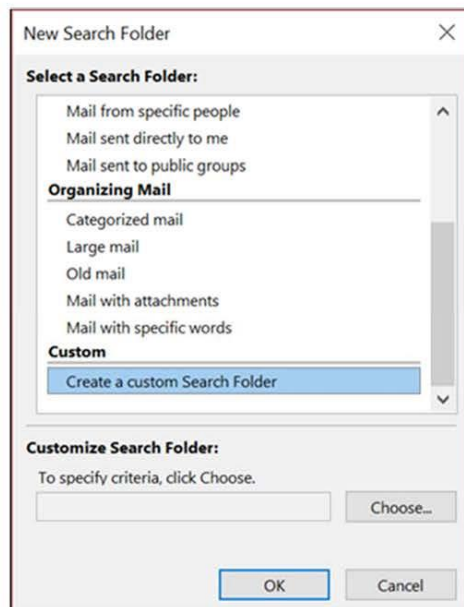
5. If you have multiple accounts in Outlook, you can specify which account to search. Use the **Search mail in box** to pick the email account you want to search, then select **OK**.

II CREATE A CUSTOMIZED SEARCH FOLDER

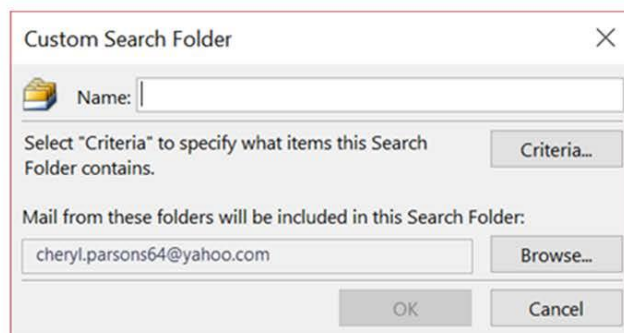
1. Select the **Folder** menu.
2. In the **New** group, select **New Search Folder**.

Keyboard shortcut To create a Search Folder, click Ctrl+Shift+P.

3. From the **Select a Search Folder** list, scroll down to the bottom and then click **Create a custom Search Folder**.



4. Under **Customize Search Folder**, click **Choose**.
5. Type a name for your custom Search Folder.



6. Click **Criteria**, and then select the options that you want.
 - The **Messages** tab contains criteria on the message content or properties, such as sender, keywords, or recipients.

A screenshot of the "Search Folder Criteria" dialog box. It has three tabs: "Messages", "More Choices", and "Advanced". The "Messages" tab is selected. Inside, there is a "Search for the word(s):" text box with a dropdown arrow, an "In:" dropdown menu set to "subject field only", two "From..." and "Sent To..." buttons with corresponding text boxes, a "Where I am:" checkbox with a dropdown menu set to "the only person on the To line", and a "Time:" section with two dropdown menus set to "none" and "Anytime". At the bottom are "OK", "Cancel", and "Clear All" buttons.

- The **More Choices** tab contains criteria on other message conditions, such as importance, flags, attachments, or categorization.
 - The **Advanced** tab enables you to make detailed criteria. Under **Define more criteria**, click **Field**, click the type of criterion that you want, and then click the specific criterion from the list. Then in the **Condition** box and the **Value** box, click the options that you want, and then click **Add to List**. Repeat for each criterion that you want to add to this search folder, and then click **OK**.
7. Click **Browse**, select the folders that you want to be searched.
 8. Click **OK** to close each open dialog box.

DELETE A SEARCH FOLDER

If you no longer need a Search Folder, you can delete it. A Search Folder is a virtual folder. Deleting a Search Folder from the folder list doesn't delete the messages displayed in the folder. If you want to delete all messages within a Search Folder, open the Search Folder, select all of the messages, then click Delete on your keyboard.

To delete a search folder, use the following steps.

1. In the Folder List, select the down arrow next to the word **Search Folders** if needed to expand your list of Search Folders.
2. Right-click the Search Folder you want to delete and choose **Delete Folder**.



Important: Deleting a Search Folder doesn't delete any messages. Deleting a folder that's not a Search Folder will delete both the folder and the messages inside the folder.





APPENDIX A: SEARCH REFERENCE TABLES

The following table shows you some examples of searches you might find useful. In addition to these examples, you can use AND, NOT, OR, <, >, =, and other operators to refine your search. Operators should be typed in uppercase letters.

Type this	To find this
bob	Items containing <i>bob</i> , <i>bobbinbobby</i> , <i>BOBBY</i> , <i>BoBby</i> , or any other combination of uppercase and lowercase letters. Instant Search is not case sensitive. This will NOT find items containing <i>abcBOBdef</i> , or <i>123bob</i> .
bob moore	Items containing <i>bob</i> , along with all of the variations listed in the previous row, or <i>moore</i> , along with any other words that contain <i>moore</i> , but not necessarily in that order.
bobby AND moore	Items containing both <i>bobby</i> and <i>moore</i> , but not necessarily in that order. Note that logical operators such as AND, NOT, and OR must be in uppercase letters.
bobby NOT moore	Items containing <i>bobby</i> , along with all variations listed in the first row of the table, but not <i>moore</i> .
bobby OR moore	Items containing <i>bobby</i> , along with all variations listed in the first row of the table, <i>moore</i> , or both.
"bob"	Items containing the exact phrase <i>bob</i> and not the variations such as <i>bobby</i> or <i>bobbin</i> . To search for an exact string, you must use quotation marks.
from:"bobby moore"	Items sent from <i>bobby moore</i> . Note the use of double quotes so that the search results match the exact phrase within the quotes. You can also type <i>from:</i> and then the first few letters of a contact's name and Outlook will suggest a list of contacts for you to select.
from:"bobby moore" about:"status report"	Items sent from <i>bobby moore</i> where <i>status report</i> appears in the subject line, body, or attachment contents. Note the use of double quotes so that the search results match the exact phrase within the quotes.



Type this	To find this
hasattachment:yes	Items that have attachments. You can also use hasattachment:true to get the same results.
attachments:presentation.pptx	Items that have attachments named <i>presentation.pptx</i> or an attachment that contains <i>presentation.pptx</i> within its contents.
subject:"bobby moore"	Items whose subject contains the phrase <i>bobby moore</i> .
cc:"bobby moore"	Items in which the display name <i>bobby moore</i> is on the Cc line.
cc:bobbymoore@contoso.com	Items in which the e-mail address <i>bobbymoore@contoso.com</i> is on the Cc line.
bcc:bobby	Items in which <i>bobby</i> is on the Bcc line.
category:red	Items that contain a category name that includes the word red. For example "Red category" or "Redo" or "Redundant."
message size:<10 KB	Items whose size is less than 10 kilobytes. Note the use of the "less than" comparison operator (<).
messagesize:>5 MB	Items whose size is larger than 5 megabytes. Note the use of the "greater than" comparison operator (>).
received:=1/1/2016	Items that arrived on 1/1/2016. Note the use of the "equals" comparison operator (=).
received:yesterday	<p>Note: The received ribbon button has been replaced with a date selector under Advanced Search. Users can still manually enter dates in the main search box.</p> <p>Items that arrived yesterday. Instant Search also recognizes the follow date values:</p> <p>Relative dates: For example, <i>today, tomorrow, yesterday</i></p> <p>Multi-word relative dates: For example, <i>this week, next month, last week, past month, coming year</i></p> <p>Days: <i>Sunday, Monday ... Saturday</i></p> <p>Months: <i>January, February ... December</i></p>



Type this	To find this
received:last week	Items that arrived last week. Note that if you run this query again a month from now you will obtain different results because it is a time relative query.
due:last week	Items that are flagged for follow up a due date.
message size:tiny	Items whose size is less than 10 kilobytes
message size:small	Items whose size is between 10 and 25 kilobytes
message size:medium	Items whose size is between 25 and 100 kilobytes
message size:large	Items whose size is between 100 and 500 kilobytes
message size:verylarge	Items whose size is between 500 kilobytes and 1 megabyte
followupflag:follow up	Items that are flagged using the Follow Up flag.
message size:enormous	Items whose size is larger than 5 megabytes
hasflag:true	Items that are flagged for follow up.
from:bobby (received:1/7/17 OR received:1/8/17)	Items from <i>bobby</i> that arrived on either 1/7/17 or 1/8/17. Note the use of parentheses to group the dates.
received>=10/1/16 AND received<=10/5/16	Items that arrived between 10/1/16 and 10/5/16. Note: For received ranges, do not use a colon.
received>10/1/16 AND received<10/5/16	Items that arrived after 10/1/16 but before 10/5/16. Note: For received ranges, do not use a colon.
sent: yesterday	Returns all items sent yesterday (by anyone). This search will return items you sent to others and items others sent to you.
to:bobby	Items that you sent to <i>bobby</i> when you are searching in the Sent Items folder.
read:no	Items that have not been read. You can also use read:false to get the same results.
subject:status received:May	Items received from anyone during the month of May (any year) where the subject contains <i>status</i> .



Calendar Searches

The following searches will only return the proper results when run from a Calendar folder.

Type this	To find this
startdate:next week subject:status	Calendar items next week where the subject contains status.
is:recurring	Calendar items that are recurring.
organizer:bobby	Calendar items where <i>bobby</i> is the organizer.

Contact Searches

The following searches will only return the proper results when run from a Contacts folder.

Type this	To find this
firstname:bobby	Contacts that contain <i>bobby</i> in the First Name field.
lastname:moore	Contacts that contain <i>moore</i> in the Last Name field.
nickname:bobby	Contacts that contain <i>bobby</i> in the Nickname field.
jobtitle:physician	Contacts that contain <i>physician</i> in the Job Title field.
businessphone:555-0100	Contacts that contain <i>555-0100</i> in the Business Phone field.
homephone:555-0100	Contacts that contain <i>555-0100</i> in the Home Phone field.
mobilephone:555-0100	Contacts that contain <i>555-0100</i> in the Mobile Phone field.
businessfax:555-0100	Contacts that contain <i>555-0100</i> in the Business Fax field.
businessaddress:(4567 Main St., Buffalo, NY 98052)	Contacts that contain <i>4567 Main St., Buffalo, NY 98052</i> in the Business Address field. Note the use of parentheses to enclose the address.
homeaddress:(4567 Main St., Buffalo, NY 98052)	Contacts that contain <i>4567 Main St., Buffalo, NY 98052</i> in the Home Address field. Note the use of parentheses to enclose the address.



Type this	To find this
businesscity:buffalo	Contacts that contain <i>buffalo</i> in the Business City field.
businesspostalcode:98052	Contacts that contain <i>98052</i> in the Business Postal Code field.
street:(4567 Main St)	Contacts that contain 4567 Main St in the Business Address Street field. Note the use of parentheses to enclose the address.
homestreet:(4567 Main St)	Contacts that contain 4567 Main St in the Home Address Street field. Note the use of parentheses to enclose the address.
birthday:6/4/1960	Contacts that contain <i>6/4/1960</i> in the Birthday field.
webpage:www.contoso.com	Contacts that contain the URL <i>www.contoso.com</i> in the Web Page Address field.



APPENDIX B: USEFUL TRAINING LINKS (VIDEOS AND ADDITIONAL TRAINING MATERIALS)

Please copy and paste the link in the browser if didn't work by clicking it.

Search and Filter Emails	Search and filter email - Outlook (microsoft.com)
Use Instance Search to find a message	Video: Use Instant Search to find messages and text - Outlook (microsoft.com)
Narrow your Search Results	Video: Narrow your search results - Outlook (microsoft.com)
Search for email, Contacts and events	Search for email, contacts, and events - Office Support (microsoft.com)
Outlook Training	Outlook training - Office Support (microsoft.com)

GROUPWISE SEARCH PROCESS

2

STATEMENT OF UNDERSTANDING:

1. Close your personal mailbox and NOTIFY BEFORE you log into the mailbox being audited.
2. When performing an AUDIT SEARCH, the searches MUST BE PERFORMED WHILE DIRECTLY LOGGED INTO THE MAILBOX BEING AUDITED TO ENSURE ACCURACY.
3. PROXY ACCESS IS NOT SUFFICIENT .
4. If an ARCHIVE EXISTS as well as a live mailbox, this process will have to be performed on BOTH message stores.

The STEPS INVOLVED when performing an Audit Search in GroupWise are:

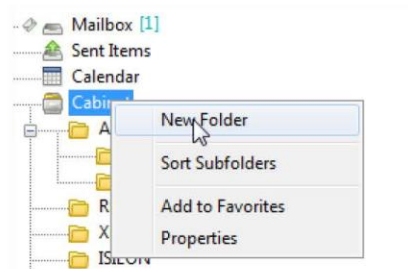
STEP 1 – CREATE YOUR STORAGE FOLDER STRUCTURE

Storing your search results in specific folders helps maintain an audit trail and allows the search results to be re-visited at any time. The folder structure should be as follows:

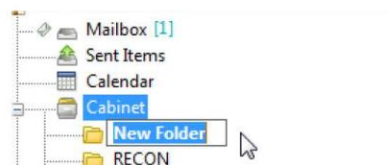


You first create an upper level (i.e. AUDIT2015) folder to hold all of your search result folders. For example, if the search criteria is “ABC Industries” then create a folder under AUDIT2015 called the same. Try to keep the folder names exactly the same as the search criteria .

To create a folder under your cabinet perform the following steps:



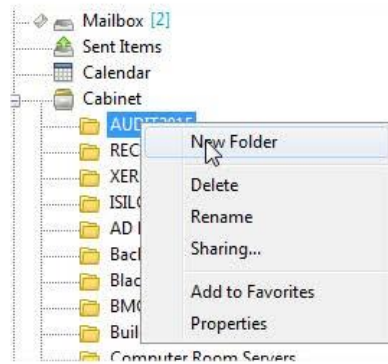
Right-click on your Cabinet and select New Folder.



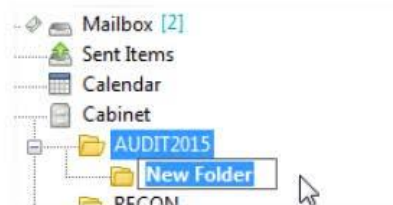
Name the folder **AUDIT2015** and press Enter .

4

Now you want to create your subfolders and name them to match your search criteria.



Right-click on AUDIT2015 and select New Folder.



If the search criteria is **“ABC Industries”** then name the subfolder the same. Perform this task until you have a folder for each of the search criteria you will be requesting.



STEP 2 – CONFIGURE YOUR SEARCH CRITERIA USING GLOBAL FIND

You will want to perform a Global Find. This is the best Find to use because it searches for the key word(s) everywhere in your mailbox. The places a Global Find searches in includes :

TO field FROM Field BC Field CC Field

SUBJECT Line

Message BODY

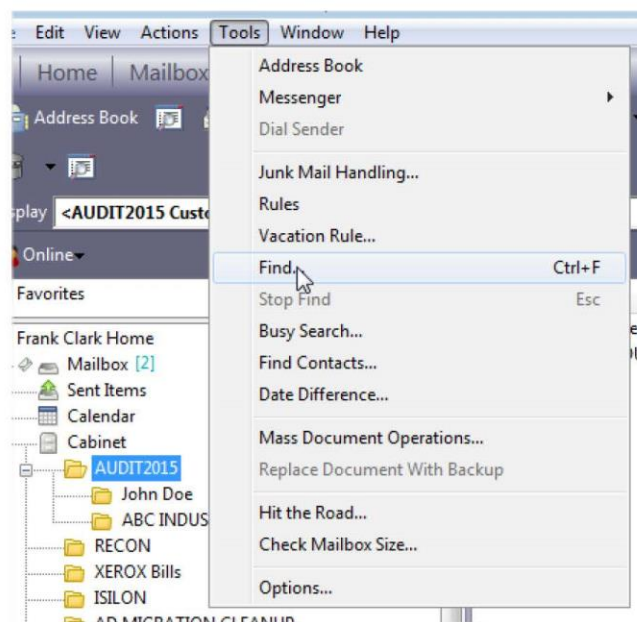
Message PROPERTIES

ATTACHMENTS (Please NOTE that image files are not searchable)

SENT Items

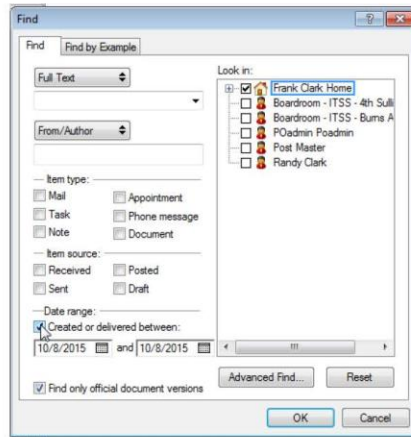
ENSURE THE FOLDER YOU ARE DRAGGING AND DROPPING TO IS VISIBLE IN THE FOLDER LIST.

To initiate a Global Find :

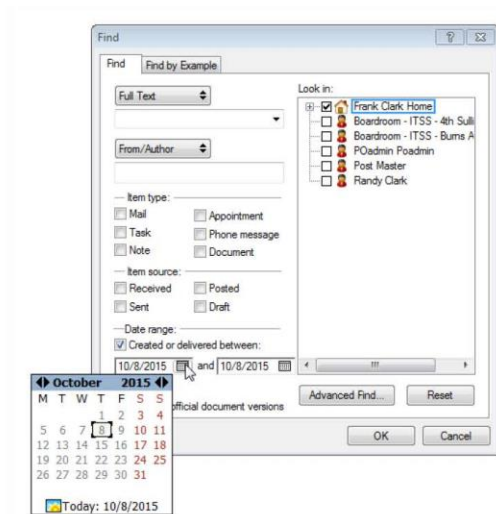


Click on Tools in your menu bar and select Find .

6

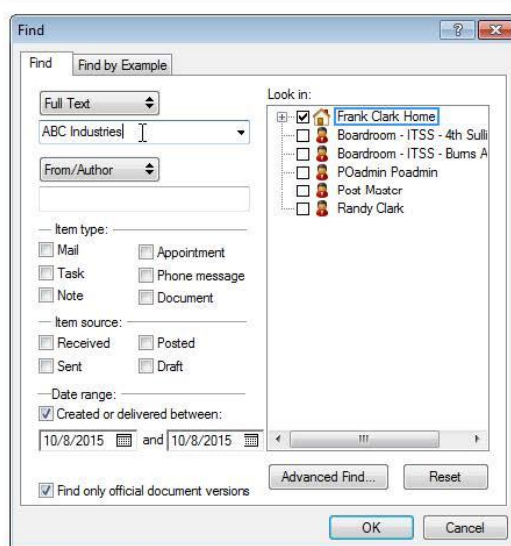


Click the box at the bottom left called “Created or delivered between” so you can set the date range you want to search on. **THE DATE RANGE IS VERY IMPORTANT. ENSURE IT IS CORRECT !**

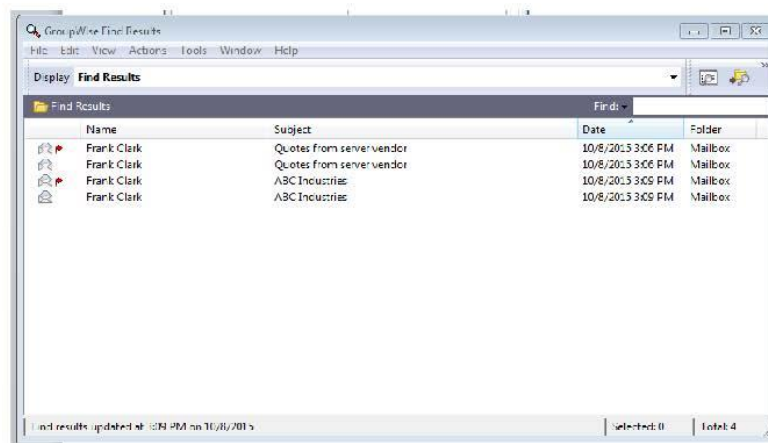


Click on the first date field to select your starting date. Use the arrows to the right of the Year to select the Year FIRST. Once set, use the arrows to the left of the Month to select your starting month, then click on the day within to complete your start date . Repeat the process to set your end date on the adjacent field.

7



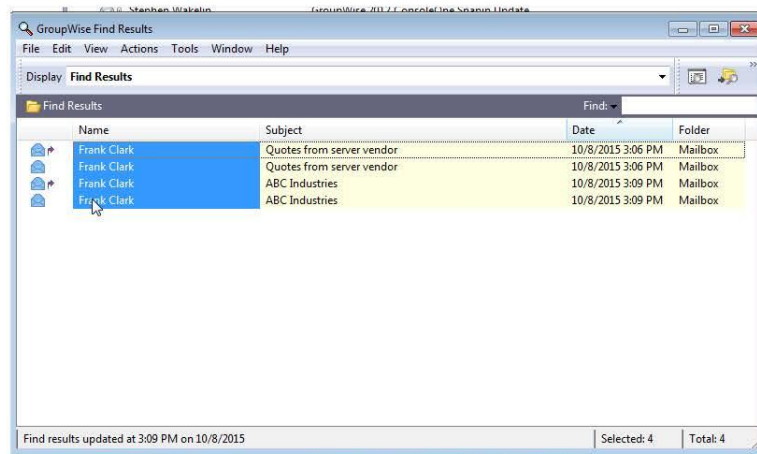
Enter your search criteria under the “Full Text” header at the top left of the Find dialog box. You will notice that the “Home” box is ticked in the “Look in” window on the right. This lets you know it is searching everywhere in the mailbox. Click OK.



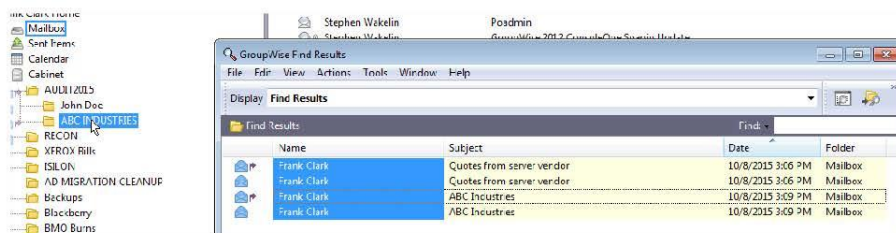
Your results appear in a “Find Results” box.

STEP 3 - DRAG AND DROP SEARCH RETURN TO STORAGE FOLDER

You will now want to put your search results into the matching folder. To do this you:



Hold down the “Shift” key and left-click on the first item in the list. While continuing to hold down the “Shift” key, scroll to the bottom of the results and left-click on the last item. This will select the entire range of resulting items. You can now release your keys.



Holding down your left mouse button, move your pointer over and high-light the folder you want to copy the items to. Once selected, release the mouse button and the files will be deposited.

You can now close the “Find Results” window and repeat steps 2 and 3 for the next search criteria.

9

Please conduct a second search using - Find By Example and enter in the search criteria.

Micro Focus GroupWise - Mailbox

File Edit View Actions Tools Window Help

Find

Find Find by Example

Item type: Mail

☒ Received ☐ Sent ☐ Personal ☐ Draft

From: John Doe

To, CC:

Subject:

Message, Attachments: Audit Report

☒ Find items in the trash

OK Cancel

Amanda

Guide for Printing GroupWise E-mails

Print with Disclosure in Mind

The file path that prints along the bottom of your document has been identified by ITSS **a risk to the security of the government computer system.**

Sample

File:///C:/users/.....9/10/21

It is important that you take steps to protect the computer system by removing the file path from all documents prior to sharing them outside of government. It is much easier to avoid printing the file path using the below instructions.

1. In the GroupWise Mailbox, Open up a message.
2. Select View and make sure Plain Text is chosen.
3. Click File and then Print.
4. Select Print Options.
5. Remove the Print Header box in the Header & Header fonts area

For more information about the above, or protecting government's computer system contact:

ITSS service centre
Tel: 902 368 3600
E-mail: servicesservice@gov.pe.ca

MEMORANDUM

TO: [FOI Coordinator – name and title]
FROM: [Designated Public Body Head – name and title]
RE: Delegation of powers and functions under the *Freedom of Information and Protection of Privacy Act R.S.P.E.I. 1988, c. F-15.01*

Whereas the [designated public body] has the following duties under the *Freedom of Information and Protection of Privacy Act R.S.P.E.I. 1988, c. F-15.01*:

- Duty to assist applicants (excluding the duty to conduct a reasonable search), section 8(1);
- Duty to respond to a request without undue delay, section 9(1);
- Duty to provide access to a record, section 11;
- Duty to provide an applicant with information about time extension, section 12(4);
- Duty to notify the applicant that a request has been transferred to another public body, sections 13(2)(a) & 34(8)(a);
- Duty to respond within 30 days to a request transferred from another public body, sections 13(2)(b) & 34(8)(b);
- Duty to give notice to a third party where considering giving access to third party information, section 28(1);
- Duty to give notice to an applicant regarding notice to third party, section 28(4).

In order to perform these duties, I hereby authorize you to assist with these duties and delegate the following powers and functions vested in me pursuant to the *Freedom of Information and Protection of Privacy Act* to you:

Right of Access

- Power to declare a request abandoned for lack of response, section 7(4);
- Power to extend the time limit for responding to a request, section 12(1) & (3);
- Power to request Commissioner's permission for extension of the time limit for responding to a request, section 12(1) & (2);

- Power to transfer a request to another public body, sections 13(1) & 34(7);

Third Party Consultation

- Power to give notice to a third party where not considering giving access to third party information, section 28(2);

Fees

- Power to require an applicant to pay fees for services, section 76(1).

All requests made pursuant to the *Act*, and all directions under the *Act*, are to be processed in accordance with the *Freedom of Information and Protection of Privacy Act*.

Dated this _____ day of **[month, year]**

[Head name and designated public body]

cc: Denise Doiron, Office of the Information and Privacy Commissioner