

2025 FOIPP ACT REVIEW

Recommendations from the Office of the Information and
Privacy Commissioner



OIPC

Office of the Information &
Privacy Commissioner of PEI

TABLE OF CONTENTS

Page

I. Introduction	1
II. Addition of Public Bodies – Municipalities	2
III. Mandatory Breach Notification	5
IV. Mandatory Privacy Impact Assessments	6
V. Production of Records for Review, section 53	7
VI. Other Amendments for Consideration	10
Subsection 12(1) [extension of time]	10
Section 19 [intergovernmental relations]	11
Section 34 [request to correct]	12
Section 61 [requesting a review]	12
Section 75 [offences]	14
Section 52 [request to disregard]	15
Schedule I – Table of Recommendations	16

I. Introduction

The *Freedom of Information and Protection of Privacy Act* (“*FOIPP Act*”) was proclaimed in November of 2002. Since that time, the number of access requests made to public bodies subject to the *FOIPP Act* have increased steadily year after year. Transparency, accountability, and trust are more important now than they ever have been before, which makes access to information more important than ever.

In addition to access to information, public bodies have an obligation to protect personal information in their custody and control under the *FOIPP Act*. There is increasing concern about personal privacy, particularly in light of the number of large data breaches experienced in recent years. The Office of the Information and Privacy Commissioner (“OIPC”) has observed an upward trend in the number of complaints regarding public bodies’ handling of personal information.

As a former Commissioner remarked, our *FOIPP Act* is well-written, and has proven to be effective¹. However, there have been many changes in the areas of access to information and protection of privacy since the *FOIPP Act* was first proclaimed, and even since the last review in 2017. Some challenges have arisen, both here and across the country. As a result, there are some amendments to the *FOIPP Act* the OIPC encourages this Committee and the Legislature to consider, with a view to improving access to information and the protection of personal information by public bodies in our province.

The recommendations in this report are based on our internal review of the *FOIPP Act*, our experiences with administering the *FOIPP Act*, discussions with our counterparts in other jurisdictions, and information the OIPC has gathered since the last review.

The OIPC is not only a stakeholder but has a unique role in a legislative review. We work with this law daily and may be able to answer questions about interpretations, how various provisions operate, and respond to proposals of other stakeholders. If the Committee considers other amendments to the *FOIPP Act* not described in this report, we request the opportunity to provide comment on them.

I thank the Committee for the invitation to make recommendations.

Denise N. Doiron
Information and Privacy Commissioner

¹ [oipc-FOIPP-Act-recommendations.pdf](#)

II. Addition of Public Bodies - Municipalities

In the latest amendments to the *FOIPP Act*, which were proclaimed in 2018, the Legislature added four municipalities to the list of public bodies subject to the *FOIPP Act* (Charlottetown, Summerside, Cornwall and Stratford).

Before this, the public did not have a legislated right to access information in the custody or control of any municipalities, and municipalities were not subject to the same privacy obligations as public bodies for personal information in their custody or control. The *Municipal Government Act* was enacted in December 2017, which requires councils to create bylaws to address access to information and protection of privacy.

Issue: While there is now a requirement for all municipalities to create bylaws to address access to information and protection of privacy, the statutory standard is far less detailed than the *FOIPP Act*. There is no independent oversight of the bylaws related to information access and protection of privacy, or a municipality's compliance with them. There is no recourse for individuals who have a complaint about a municipality's decision on access to information, and limited recourse for individuals who have a complaint about a municipality's privacy practices.

The OIPC has received complaints from the public about various municipalities that are not among the four added during the last review. However, we do not have the jurisdiction over access to information and protection of privacy by municipalities that are not subject to the *FOIPP Act*, and there is no independent review. Because of the limited provisions of the *Municipal Government Act* regarding municipalities' information practices, the lack of independent oversight, and the importance of accountability and responsibility to the public, we strongly encourage the Legislature to consider adding all municipalities under the *FOIPP Act*.

In 2021², the populations of the larger municipalities in Prince Edward Island were:

Charlottetown	38,809
Summerside	16,001
Stratford	10,927
Cornwall	6,574
Three Rivers	7,883
Kensington	1,812

² <https://www12.statcan.gc.ca/census-recensement/2021/dp-pd/prof/index.cfm?Lang=E>

As population growth increases, it is important for transparency, accountability and trust for municipalities to be subject to the same laws and have consistent application and enforcement. For this reason, we consider it important for all municipalities to be subject to the *FOIPP Act*.

We recognize that it may not be feasible for all municipalities to be added all at once, and that a phased-in approach may be preferable. We are recommending at least two municipalities be added to the list of designated local public bodies at this time: Kensington and Three Rivers.

Kensington

The Town of Kensington is not our largest municipality, but it has its own Police Department, currently consisting of a Police Chief, Deputy Chief, two full-time constables, and three part-time constables.

When the *FOIPP Act* was last reviewed, PEI and Saskatchewan were the only two provinces that did not have municipal police forces subject to legislation similar to the *FOIPP Act*. In 2018, Saskatchewan added all police services to their equivalent legislation³.

PEI has three municipal police forces, in the City of Charlottetown, City of Summerside, and Town of Kensington. When the 2018 amendments were made to the *FOIPP Act*, the City of Charlottetown and City of Summerside were added as local public bodies, and their police forces became subject to the *FOIPP Act*.

The Town of Kensington was not included in the list of local public bodies that became subject to the *FOIPP Act*. This means that while the Kensington Police Department operates in the same manner as other police forces in the province, it is not subject to the same legislated obligations of access to information and protection of personal privacy as the other police forces. In fact, we were unable to find any other police force in Canada that was not subject to specific *FOIPP Act*-equivalent legislation. (The RCMP are subject to the federal *Privacy Act* and *Access to Information Act*.)

Kensington has a bylaw addressing access to information and protection of privacy in general, as required under the *Municipal Government Act* and its regulations, but they do not specifically address law enforcement matters. In addition to protection of personal privacy and access to information – both personal information and public information – the *FOIPP Act* permits a public body to withhold information to protect some legitimate law enforcement interests.

³ [L27-1 \(3\).pdf](#) *Local Authority Freedom of Information and Protection of Privacy Act*, Chapter L-27.1 of the Statutes of Saskatchewan, 1990-91, at subclause 2(1)(f)(viii.1)

Adding Kensington to the list of designated local public bodies under the *FOIPP Act* will permit the Kensington Police Department to protect information related to law enforcement matters. It will also enhance the Town's access to information and protection of privacy requirements, provide more clarity around the Town's obligations and citizens' rights, and facilitate independent oversight of the Town's access to information and protection of privacy practices.

Three Rivers

The Town of Three Rivers did not exist when the *FOIPP Act* was last amended. Three Rivers incorporated in September 2018, a few months after the last amendments to the *FOIPP Act* were proclaimed, and became one of the larger municipalities in the province. It amalgamated the communities of Montague, Georgetown, Lower Montague, Brudenell, Cardigan, Lorne Valley, Valleyfield, and portions of unincorporated areas adjacent to these locations.

Although one of the larger municipalities in the province, it is not subject to the same legislative provisions as the other larger municipalities. The Town of Three Rivers being added to the list of designated public bodies under the *FOIPP Act* will ensure consistency of access to information and protection of privacy obligations across the larger municipalities in the province, and facilitate independent oversight.

Recommendation: Add the Town of Kensington and Town of Three Rivers as designated municipalities. This could be done either by a) adding them to the definition of "designated municipality" under subsection 1(b.2) of the *FOIPP Act*; or b) by designating them as a "designated municipality" under the *FOIPP Act* regulations by adding them to Part 2 of Schedule 1 in the *FOIPP Act* regulations.

An alternative option for consideration is to add any municipal police force to the definition of "Local Public Body" under subsection 1(e.1) as follows:

1. In this act

...

(e.1) "local public body" means

(i) a designated educational body, ~~or~~

(ii) a designated municipality;

(iii) the police department established for the Town of Kensington; or

(iv) any other police department that is established for a municipality as defined in the Municipal Government Act, R.S.P.E.I. 1988, Cap. M-12.1;

Timing: When the local public bodies were added to the *FOIPP Act*, the amendments were proclaimed in June 2018, but the Legislature delayed the application of the *FOIPP Act* to the local public bodies until April 1, 2019. If the Legislature decides to add more municipalities as designated municipalities under the *FOIPP Act*, the Legislature may wish to consider a delayed statutory effective date. This would allow the added municipalities an opportunity to become familiar with their obligations under the *FOIPP Act*, ensure their bylaws and practices are in compliance with the *FOIPP Act*, and train their personnel accordingly.

III. Mandatory Breach Notification

Although public bodies have an obligation under the *FOIPP Act* to protect personal information in their custody or control, there are times when things happen that lead to unauthorized disclosure of or access to personal information, such as when personal information is stolen, lost, disposed of without authority, or disclosed to or accessed by an unauthorized person. This is commonly called a “breach”.

Privacy breaches or data breaches happen for a variety of reasons, some unintentional and some due to intentional acts of internal or external sources. Sometimes, a breach occurs due to an unfamiliarity with what is or is not authorized. Whether intentional or not, the result is that personal information of individuals is compromised.

Issue: It is likely not a surprise to most people that breaches occur. What might be surprising, however, is that there is no requirement under the *FOIPP Act* for public bodies to report to individuals or to our office that a breach has occurred.

We are aware that breaches are occurring, but we do not have a sense of how many have occurred. We have noted an increase in public bodies taking a proactive approach and voluntary reporting breaches to our office. But, while some public bodies voluntarily report breaches, we do not know if they are doing so in every instance. We are also aware that many public bodies do not report breaches to our office or notify affected individuals.

Recommendation: We recommend adding a requirement for public bodies to notify our office and affected individuals if their personal information was lost, stolen, disposed of without authority, or disclosed to or accessed by an unauthorized person.

PEI's *Health Information Act* has a mandatory breach reporting requirement (section 36), which requires health information custodians to notify an affected individual and the OIPC if there is a breach, with the exception of when a custodian believes the breach will not have an adverse impact.

Adding a mandatory breach reporting requirement to the *FOIPP Act* will:

- a) harmonize the *FOIPP Act* with similar provisions in the *Health Information Act*;
- b) permit people who are affected by a breach to take measures to reduce or mitigate the risk of harm;
- c) enable the OIPC to assess whether public bodies are notifying individuals effectively, and to review whether public bodies are containing the breaches, mitigating the risk of harm to individuals, identifying any gaps or weaknesses that may have contributed to the breach and implementing measures to prevent similar breaches in future;
- d) increase transparency and accountability of public bodies and public trust in those public bodies;
- e) assist in potentially identifying systemic weaknesses in the protection of personal information; and
- f) bring Prince Edward Island in line with best practices and public expectations for protection of privacy.

IV. Mandatory Privacy Impact Assessments

Privacy impact assessments are tools used when considering new initiatives before they are implemented, to ensure such initiatives are compliant with privacy rules and have adequate security measures in place. This could apply to a new program that involves the collection, use, access to or disclosure of information, the implementation of new technology, such as an information management system, application, or service delivery tool, or a substantial change in existing collection, use, access to, or disclosure of personal information.

The public increasingly expects information and services to be accessible online or through other technological avenues, and public bodies are always looking for new and improved ways of delivering services, and increasing productivity and efficiency, as well as convenience and barrier-free access for the public they serve. Privacy impact assessments are increasingly more important in the face of the fast-paced development and wide-ranging availability of technology options.

Not all technology is created equal. As the use and variety of technological options available increases, the need increases for public bodies to be careful to ensure the options they choose have appropriate security measures in place to protect the personal information that public bodies have in their custody and control, and to ensure that information is not at increased risk of unauthorized collection, use, disclosure or access.

Issue: The *FOIPP Act* does not currently require public bodies to conduct privacy impact assessments, or for any privacy impact assessments that are conducted to be submitted to our office for review and comment.

Occasionally, public bodies conduct privacy impact assessments before such new initiatives, and sometimes they are submitted to our office for review and comment. However, this is done on a voluntary basis, and not always before a new initiative or technology is implemented.

Recommendation: We recommend requiring public bodies to complete privacy impact assessments when a public body is developing a new project or service that involves the collection, use, access to, or disclosure of personal information, when a public body is planning on implementing new technology that will involve the collection of, or storage of collected, personal information, or implementation of a new initiative where the public body plans to disclose personal information without consent or outside of the province, or any significant change to the collection, use or disclosure of personal information.

We further recommend that, in addition to a requirement for public bodies to conduct privacy impact assessments, that there be a requirement for them to provide the privacy impact assessments to our office for review and comment, prior to the implementation of any such program, service, technology or initiative.

The *Health Information Act* (section 25) requires health information custodians to conduct a privacy impact assessment and submit it to our office for review and comment in specified circumstances. If the Legislature accepts this recommendation and decides to add a mandatory privacy impact assessment provision to the *FOIPP Act*, they may wish to consider a provision similar to what is set out in section 25 of the *Health Information Act*.

V. Production of Records for Review, Section 53

Public bodies may withhold requested information from an applicant if the information is subject to legal privilege. One of the primary roles the Legislature has tasked our office with is, when there is a complaint, to review whether a public body is authorized to withhold information.

When conducting a review, section 53 of the *FOIPP Act* authorizes the Commissioner to require any record to be produced to the Commissioner and requires a public body to produce any such record within 10 days. This is an important provision because, when a public body refuses to disclose information to an applicant, and an applicant asks for a review of that decision, the only way we can determine if the public body properly applied an exception to their disclosure obligations under the *FOIPP Act* is to review the information that was refused. This is a vital part of the Commissioner's function, and the only way independent oversight can be carried out.

Issue: There is a class of records that is exempt from the authority to require production of records in a review under the *FOIPP Act*, records over which a public body claims legal privilege, such as solicitor-client privilege.

The courts have given broad protections to records created in preparation for a legal proceeding or when someone seeks legal advice, based on the broad public policy objective of encouraging people to be forthright with their legal counsel when seeking legal advice. This applies equally to public bodies. Section 25 of the *FOIPP Act* permits public bodies to refuse to disclose information over which legal privilege, including solicitor-client privilege and litigation privilege, is claimed.

Subsection 53(3) states that when the Commissioner requires a record to be produced, a public body is required to produce it within 10 days “despite any other enactment or any privilege of the law of evidence”. However, in considering a similar provision in the Alberta *FOIPP Act* in 2016, the Supreme Court of Canada found that the words “privilege of the law of evidence” was not sufficiently clear, explicit and unequivocal to show a legislative intent to set aside solicitor-client privilege⁴. In order for such a provision to authorize the Commissioner to compel the production of documents over which solicitor-client privilege is claimed, the provision must clearly specify that this authority applies despite any “legal privilege”.

⁴ *Alberta (Information and Privacy Commissioner) v. University of Calgary*, [2016] 2 SCR 555, 2016 SCC 53 (CanLII) <https://canlii.ca/t/gvskr> at paragraphs 44 and 53.

The ability to review records that a public body has refused to disclose to an applicant is an integral part of our independent oversight function. If we are not able to review the records to determine whether an exception was properly applied, it becomes quite difficult to determine whether a public body is complying with their obligations of access to information.

We have been seeing an increase in public bodies asserting solicitor-client privilege over records and refusing to disclose the records to applicants. The volume of records over which public bodies are claiming legal privilege is increasing as well. Although public bodies may produce, during a review, records over which they claim solicitor-client privilege, they are not required to do so and usually refuse.

If a public body refuses to produce to us records over which they are claiming solicitor-client privilege, they are supposed to give us an affidavit explaining the nature of the records and providing sufficient information for us to assess whether solicitor-client privilege applies. However, such affidavits tend to lack sufficient detail for us to make such assessments. We have commented in several orders on the inadequacy of public bodies' affidavit evidence.

Decisions of our office, or any tribunal or judge for that matter, are only as good as the evidence put before them. If public bodies do not provide us with the records themselves or they give us insufficient evidence, we are left in the position of having to order the disclosure of records because we cannot determine that the exception does apply.

This is not unique to Prince Edward Island. All jurisdictions in Canada are struggling with this same issue and have been calling on their respective governments to amend their legislation to allow the oversight authorities to compel the production of such records for the purposes of review. British Columbia is an exception because they have incorporated into their legislation reference to production of records over which solicitor-client privilege is claimed⁵.

Recommendation: Amend section 53 of the *FOIPP Act* to expressly authorize the Commissioner to compel the production of and review records over which a public body claims legal privilege, using clear and unambiguous language, in order to determine whether this exception to disclosure has been properly asserted.

⁵ British Columbia *Freedom of Information and Protection of Privacy Act* [RSBC 1996] Chapter 165, [Freedom of Information and Protection of Privacy Act](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_04#section44) (https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_04#section44)

Former Commissioner Karen A. Rose had requested this amendment in the last review, as well, but it was not accepted. Our office was not informed of the reason for this decision, but it is possible that lawyers or public bodies may be concerned that disclosing records over which they claim solicitor-client or other legal privilege may cause privilege to be waived. However, it is our view that this is not substantiated. Any such provision can, and should, specifically state that the privilege is not affected by the requirement to produce such records to our office.

We would also point out that the public bodies' interests are further protected by:

- (a) subsection 53(5), which requires that we return any record produced once a review or investigation is completed;
- (b) section 55, which provides that any information supplied or any record produced during an investigation or review is privileged in the same manner as if it were a proceeding in a court;
- (c) section 55.1, which states that the Commissioner is not compellable to produce in a civil proceeding any records received in the course of their functions under the *FOIPP Act*; and
- (d) subsections 56(1) and 56(3), which require that the Commissioner not disclose any information obtained in performing their functions under the *FOIPP Act* [ss. 56(1)], and requires the Commissioner when conducting a review not to disclose any information a public body would be required or authorized to refuse to disclose [ss. 56(3)].

If the Legislature decides to accept this recommendation and add such a provision to the *FOIPP Act*, we would be pleased to work with Legislative Counsel to ensure the wording is sufficient to protect the legal privilege afforded to public bodies, while at the same time ensuring the Commissioner has sufficient authority to carry out the independent oversight mandate in the *FOIPP Act*.

VI. Other Amendments for Consideration

In addition to the recommendations for more extensive amendments set out herein, we have a few other recommendations for amendments we would like to offer for the Legislature's consideration.

A. Subsection 12(1) – Extension of Time to Respond

Subsection 12(1) authorizes a public body to extend their time for responding to a request for up to 30 days, provided one of four conditions applies. A public body may ask the Commissioner for permission extend for longer than 30 days for any of these four reasons, or if an applicant (or two or more applicants working for the same organization or who work in association with each other) has made multiple concurrent requests to the public body.

Issue: The Commissioner does not have authority to give a public body permission to extend their time more than 30 days in any other circumstance, such as if an applicant consents to a longer time, or if there are unexpected and unavoidable business disruptions (e.g. adverse weather events, extended power outages, cyber security events, security incidents, public health orders).

It would be helpful if section 12 provided some flexibility for the Commissioner to permit a public body to extend their time to respond to an applicant for more than 30 days in other circumstances.

Recommendation: We recommend amending subsection 12(1) to give the Commissioner the authority to permit a public body to extend their time to respond to an applicant for longer than 30 days if the applicant consents to the extension, or if, in the opinion of the Commissioner, a longer time is reasonable in the circumstances.

B. Section 19 – Disclosure Harmful to Intergovernmental Relations

- (i) Clause 19(1)(a) is a discretionary exception if disclosure of information could reasonably be expected to harm relations between the Government of Prince Edward Island and several specified types of government. The list does not include indigenous governments or apply to inter-municipal relationships.

Recommendation: Consider adding indigenous governments to clause 19(1)(a); and adding a new clause to subsection 19(1) to protect inter-municipal government relationships.

- (ii) Public bodies are implicitly authorized to consult with other governments, with respect to concerns about intergovernmental relations under section 19. The issue is that this provision does not have a timeline within which the consulted party must give a reply to the public body. We have noted increasing number of extension requests from public bodies to extend their time to respond to an applicant because they are waiting for a response to a consultation with another government/agency.

Consultations between public bodies is generally not an issue. However, federal government departments typically have been taking anywhere from a few months to a year or more, depending on the department and number of pages being consulted about, before responding. This is an issue across Canada.

Recommendation: We recommend adding a response time for another government to respond to a public body's consultation under section 19.

C. Section 34 – Correction of Personal Information

An individual has a right to request that a public body correct personal information in the public body's custody or control if the individual believes there is an error or omission in the individual's personal information. A public body does not have to make the correction but, if they decide not to, they must annotate or link the "part of the requested correction that is relevant and material to the record in question."

This can be a difficult process, depending on the length of the request, the amount of personal information the individual is asking to be corrected, how many records must be linked or annotated, and the ease of making the links or annotations.

The *Health Information Act* also permits an individual to request corrections to their personal health information, but the process is slightly different. Instead of requiring a link or annotation, it entitles an individual to file a concise statement of disagreement stating the correction requested and the reason for the correction. This statement must be added to the record of the individual's information, so it can be read with and form part of the record, or be cross-referenced to it.

A process similar to what is set out in the *Health Information Act* would take some of the workload off of a public body, and would permit individuals to concisely express their own personal information as they wish.

Recommendation: We recommend amending section 34 to remove the requirement for a public body to annotate or link a requested correction to an individual's personal information if the requested correction is not made, and adding the ability for an individual to file a concise statement of disagreement stating the correction requested and the reason for the correction, which must be added to the record of the individual's personal information.

D. Section 61 – Time to Request a Review

The wording of subsection 61(2) about the time limitations for when someone can ask the Commissioner for a review could be clearer. Someone can ask for a review of a public body's refusal to grant access to a record or to correct personal information [ss. 60(1)], a decision to disclose a third party's information [ss. 60(2)], when a person believes their own personal information has been collected, used, or disclosed without authority [ss. 60(3)], or a refusal to disclose personal information to a relative of a deceased person [ss. 60(4)].

Individuals will be notified of decisions about a request for access or correction, to disclosure of information about a third party, or a request by a relative of a deceased individual. In most instances, it will be clear when the limitation period starts. However, a person may not be aware that their own personal information was collected, used or disclosed in violation of Part II of the *FOIPP Act*, so determining when the limitation period for requesting a review starts may not be as straightforward.

Adding a provision to section 61 to identify that the limitation period for requesting a review under subsection 60(3) starts when the individual becomes aware that their own personal information was collected, used or disclosed in violation of Part II would add some clarity to when the limitation period starts

Recommendation: We recommend amending subsection 61(2) to specify that a request for review under subsection 60(3) must be made within 60 days after the

person becomes aware of the contravention, or any longer period allowed by the Commissioner, as set out below:

61. How to ask for a review

...

Time for request

- (2) A request for a review of a decision of the head of a public body must be delivered to the Commissioner
- (a) if the request is pursuant to subsection 60(1), ~~(3)~~ or (4), within
 - (i) 60 days after the person asking for the review is notified of the decision, or
 - (ii) any longer period allowed by the Commissioner; or
 - (b) if the request is pursuant to subsection 60(2), within 20 days after the person asking for the review is notified of the decision; or
 - (c) if the request is pursuant to subsection 60(3), within
 - (i) 60 days after the person becomes aware of the contravention; or
 - (ii) any longer period allowed by the Commissioner.

E. Section 75 – Offence Penalties

Section 75 of the *FOIPP Act* sets out a variety of actions that are considered offences under the legislation and sets out the maximum penalty for anyone who has been found to have violated the Act. Currently, a person who violates the *FOIPP Act* is liable on summary conviction to a maximum penalty of a fine of \$10,000. This was the maximum penalty proposed in 1997 when the original Bill was passed. In today's dollars, that would be about \$18,000, but the penalty amount has not changed.

In addition, section 75 uses the word “wilfully” to describe an action for it to qualify as an offence. Other jurisdictions that have a similar description report that it is quite difficult to prove when an action is willful. The use of this term also excludes other kinds of actions that might be in violation of the legislation but will not be considered an offence under section 75. For example, if a public body discloses personal information due to negligence, this is not a willful act and therefore would not be considered an offence. Removal of the word “wilfully” from this provision would more adequately and accurately reflect how seriously the province takes its obligations to give access to information and protect the personal information of citizens.

Recommendation: Remove the word “wilfully” from section 75, and consider increasing the maximum penalty, to impress the message to citizens, public bodies and their employees, that the province takes access and privacy seriously.

F. Section 52

Section headings in legislation are intended to be for reference only and do not form part of the enactment⁶. However, if a section heading is not clear or accurate, it can lead to confusion.

The heading for section 52 is “Power to authorize a public body to disregard questions”. This wording is inaccurate, as the provision allows the Commissioner to authorize a public body to disregard a request for access to records made under subsection 7(1). We have issued a decision which clarifies that access provisions relate to responding to requests for access to records, and a public body is not obligated to respond to an applicant’s questions.

Recommendation: We propose the heading for this section be amended to “Power to authorize a public body to disregard an access request”, to ensure accuracy and clarity.

⁶ Interpretation Act, R.S.P.E.I. 1988, Cap. I-8.1, at subsection 19(3)

SCHEDULE I

TABLE OF OIPC RECOMMENDATIONS

SECTION	RECOMMENDATION
ss. 1(b.2)	Add the Town of Kensington and Town of Three Rivers as designated municipalities
Part II - Protection of Privacy (new provision)	Add a requirement for public bodies to notify OIPC and affected individuals if their personal information was lost, stolen, disposed of without authority, or disclosed to or accessed by an unauthorized person
Part II - Protection of Privacy (new provision)	Require public bodies to complete privacy impact assessments, and submit them to the OIPC for review and comment, prior to starting new initiative, implementing new technology, or making substantial changes to current collection, use, access to or disclosure of personal information
ss. 12(1)	Add authority for Commissioner to permit a public body to extend their time to respond to an applicant for more than 30 days if the applicant consents to a longer time, or if in the opinion of the Commissioner it is reasonable in the circumstances
s. 19	a) Add indigenous governments to clause 19(1)(a); b) Add a new clause to subsection 19(1) to include inter-municipal government relations; and c) Add a response time for another government to respond to a public body's consultation under section 19
s. 34	a) Remove requirement for a public body to annotate or link a requested correction to an individual's personal information if a requested correction is not made; b) Permit an individual to file a concise statement of disagreement, stating the correction requested and the reason for the correction; and c) Require a public body to add a concise statement of disagreement to the record of the individual's personal information
s. 52	Amend the heading to "Power to authorize a public body to disregard an access"
s. 53	Add an express authorization for the Commissioner to

	compel the production of, and review, records over which a public body claims legal privilege, including solicitor-client privilege, for the purpose of conducting an investigation or inquiry (review)
s. 61	Amend subsection 61(2) to specify that a request for review under subsection 60(3) must be made within 60 days after the person becomes aware of the contravention, or any longer period allowed by the Commissioner
s. 75	a) Remove the word “willfully”; and b) Increase the maximum penalty for an offence