ABOVE BOARD

A quarterly newsletter published by
the Office of the Information and Privacy Commissioner

Volume 18, Issue 2 April 2026

Contact Information

Office of the Information and Privacy Commissioner

Mailing Address:
PO Box 13004, Station A
St. John's, NL
A1B 3V8

Telephone:

709-729-6309

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:
commissioner@oipc.nl.ca

Website:
www.oipc.nl.ca

Follow us on social media!

LinkedIn:
https://Linkedin.com/company/oipc-nl

This Issue:

Free Virtual Municipal Workshop June 10th – Register Now

OIPC is again hosting a free, half-day virtual workshop designed specifically for municipalities on June 10, 2026, from 9 a.m - 12 p.m. (Newfoundland Time). This year, we are pleased to partner with the ATIPP Office and the OCIO's Cyber Security Office.

Our presenters will explore:

- OIPC - **Time Extensions and Disregards under ATIPPA, 2015**
- ATIPP Office - **Topic Coming Soon!**
- OCIO Cyber Security Office - **Cyber Security**

This Virtual Workshop is intended for municipal staff, ATIPP coordinators, council members, and others with a professional interest in access, privacy, security, and information management issues within the municipal context.

Given the increasing expectations placed on municipalities, and the growing complexity of access requests, workplace investigations, and emerging cyber risks, we strongly encourage all municipalities to participate!

To register please visit our website at: Municipal Workshop - Office of the Information and Privacy Commissioner.

Report on the PowerSchool Privacy Breach

The PowerSchool privacy breach impacted Newfoundland and Labrador's education system, and resulted in personal information belonging to 285,158 individuals being taken by a malicious actor.

This was the personal information of not only the current generation of students and teachers, but included former teachers dating back to 2010, and all former students of our province who were enrolled as of 1995 onwards, up to the date of the breach.

Our investigation report identified significant weaknesses in oversight, governance, and information management, and provides the Department of Education and Early Childhood Development with a detailed set of recommendations to reduce risk, enhance accountability, and improve the protection of personal information entrusted to it by students, families, and educators throughout the province.

Our report is an important read for anyone concerned with privacy, risk management, and the critical importance of strengthening privacy protections within third-party service contracts.

To learn more, read the full report here: P-2026-001.pdf.

Updates

APSIM Conference

The APSIM Conference, scheduled for November 26 and 27, 2026, continues to welcome speaker proposals. This two-day in-person event will again take place at the Health Innovation Acceleration Centre in St. John's, and will bring together access, privacy, security, and information management professionals. For the latest updates and information about APSIM, please visit the Conference's official website. If you have questions, please contact APSIMconference@gov.nl.ca.

Social Media

OIPC is expanding our social media presence! OIPC NL Instagram and YouTube accounts will soon be active, along with a new social media policy.

Feedback

If you have any questions or feedback about our forms, guidelines or guidance, including suggestions on topics for guidance resources, please let us know!

OIPC Unreasonable Behaviour Policy

OIPC has implemented a new policy addressing Unreasonable Behaviour. The policy is intended to ensure a safe and respectful environment; provide clarity regarding behaviours OIPC considers unreasonable; establish a consistent, fair and transparent process for managing unreasonable behaviours; and support the efficient functioning of OIPC. This policy is available on our website.

The Unreasonable Behaviour policy applies to all OIPC staff and individuals interacting with our Office. The policy does not impact the merits of access requests, complaint investigations, or applications before OIPC. Unreasonable behaviour is conduct that, because of its nature, frequency, or severity, interferes with OIPC's ability to provide services. Behaviour may be considered unreasonable when it falls into one or more of the following categories:

- excessive or repeated demands on the time and resources of OIPC;
- excessive persistence towards OIPC;
- engaging in any form of disrespectful, aggressive or threatening interactions with OIPC staff;
- providing false, misleading, or selectively incomplete information in a manner that interferes with OIPC's services; or
- loitering, interfering or causing a disturbance.

OIPC's response to unreasonable behaviour will be limited to what is needed to prevent or mitigate the effects of an individual's unreasonable behaviour, while continuing to provide access to OIPC's services. Individuals will be informed when their behaviour is unreasonable and, in some instances, this will be followed up in writing. When required, OIPC will implement measures to mitigate or control continued unreasonable behaviour. Measures may include specifying how often the individual may contact the Office, limiting communication methods, assigning a single point of contact, specifying topics allowed for discussion (ex. declining to discuss issues repeatedly addressed or outside of office's jurisdiction), ending conversations, and more. Process responses could include discontinuing non-essential services or setting limits on process.

For any public body that is struggling with the behaviour of applicants, a resource you may find helpful is New South Wales Ombudsman's Managing unreasonable conduct by a complainant. If you are experiencing difficulties with a complainant during OIPC processes, please let your assigned Analyst know.

The Information Desk: Applications to Disregard Access Requests

This is a new column, created in response to feedback gathered during OIPC's recent survey on our guidance, newsletter, and conference. This column will put the spotlight on OIPC's internal office processes. If you have a topic you would like to see featured, let us know by emailing commissioner@oipc.nl.ca with the subject being "Above Board Feedback."

Most public body coordinators know about section 21 of ATIPPA, 2015, which allows the head of a public body, within five business days, to apply to the Commissioner for approval to disregard an access request under certain conditions outlined in that section. The form to submit an application is on our website, along with our guidance document, which explains how we interpret and apply section 21.

What many people might not know, however, is how a decision gets made by OIPC on a public body's application for approval to disregard a request. Although ATIPPA, 2015 says that the application is made to the Commissioner, as with many tasks and decisions, it is simply not possible for the Commissioner to take on every role personally, so the job of reviewing and deciding on these

applications has in practice been delegated jointly to the Senior Access and Privacy Analyst (SAPA) and Director of Research and Quality Assurance (Director).

Once your completed application form arrives at our email address commissioner@oipc.nl.ca, our administrative staff forward it to SAPA, who reviews it and conducts an initial assessment on the merits of the application. SAPA then shares that assessment with the Director. Decisions to approve or not approve an application to disregard are then made on a consensus basis between these two officials.

Often the application is relatively clear-cut in terms of providing the necessary evidence and argument to establish a case for approval to disregard. This can mean that it clearly meets our expectations (as outlined in the guidance document mentioned above) or that it clearly does not meet our expectations. Sometimes the complexity of the matter requires a more in-depth discussion between SAPA and the Director in order to arrive at a decision. In very rare cases where consensus is not achieved, they bring the matter to the Commissioner for discussion and a final decision. Given that a decision is required to be made within three business days, it is usually not practical to seek additional submissions or input from public bodies before a decision is made, although in rare cases we may reach out for clarification if needed and if time permits. The decision to approve or not approve the application is typically communicated to the public body by SAPA.

If SAPA is away from the office for any reason, the Director carries out SAPA's role and confers with the Commissioner on disregard applications. If the Director is away, SAPA confers directly with the Commissioner. Our practice is that two senior, experienced officials of the Office are always engaged in the decision-making process for every application to disregard that is submitted by a public body. We believe this is appropriate given the significance of such an application to public bodies, as well as the serious impact that a decision to disregard a request can have on an applicant.

If you have questions about disregard applications in general, please give us a call to discuss.

Ontario's Legislative Changes

In April, the Government of Ontario passed amendments to its **Freedom of Information and Protection of Privacy Act** (FIPPA). The government's news release indicates that it updated its cyber security, privacy and access framework to better align with other Canadian jurisdictions, and that the changes will support increased data security and greater privacy. Changes include:

- excluding the records of the premier, cabinet ministers, parliamentary assistants and their offices;
- requiring relevant institutions to provide reasonable, timely assistance to requesters when a request contains insufficient detail or requires further information;
- codifying the practice of releasing voluminous requests in stages while processing continues in order to get information to requesters quickly and allow more time to process requests;
- updating timelines and terminology, including extending access request response timelines to 45 business days;
- implementing mandatory cyber security practices for hospitals, school boards, children's aid societies and post-secondary institutions;

- requiring broader public sector organizations to complete cyber maturity assessments every two years, report critical incidents and designate a single point of contact in the event of a cyber security incident; and
- allowing information contained in employee accounts to move between institutions or ministries when a public sector employee moves positions.

The Information and Privacy Commissioner of Ontario expressed concern with some of the proposed amendments and challenged the assertion that those changes will better align Ontario's legislation with the rest of the country. A statement issued March 13th called the proposed retroactive exemption of the records of the premier, cabinet ministers, parliamentary assistants and their offices "alarming" and stated, "This amendment is about hiding government-related business to evade public accountability."

The statement also raised concerns about the diminished oversight role regarding the current data integration provisions in FIPPA, which provide the government with extraordinary power to link records about individuals across government departments, including health information. Prior to the amendments, such records could already be linked for a number of valid purposes, as long as there were appropriate safeguards and oversight in place.

The statement also commented on the change that sees employees retaining their email accounts when they change jobs across different government ministries. This could allow government employees to accumulate sensitive and personal information of residents as employees move on throughout their careers, even when they no longer have any legitimate need to keep it. It also complicates responses to access requests and administration of retention schedules, as records could be scattered across ministries.

The Commissioner issued a second statement on March 26th containing factual information in response to the various reasons that have since been offered for the changes. The six facts include:

1. excluding the highest levels of government records from FIPPA is not modernization;
2. personal information of constituents, confidential commercial information, and cabinet confidences are already protected under FIPPA;
3. personal emails and personal devices should never be used to conduct government-related business;
4. removing records from FIPPA would increase cybersecurity risks to these records;
5. Ontario's FIPPA is consistent with the laws of many other Canadian jurisdictions; and
6. access to information about government-related business matters to all Ontarians.

The statement concluded with the following quote from Patricia Kosseim, Information and Privacy Commissioner of Ontario:

> Taking away Ontarians' access rights — retroactively and into the future — denies them the information they need to understand government decision-making at the highest levels and hold their governments to account. Such a change would not modernize access laws, strengthen privacy, or enhance security; it would weaken transparency and accountability for generations to come. This should be concerning

> for all Ontarians, regardless of political affiliation. We urge the government to reconsider its proposal and keep public trust onside.

The Government of Ontario passed the Bill on April 23, 2026.

Statutory Review of ATIPPA, 2015 Anticipated

Section 117 of ATIPPA, 2015 establishes that a review will be held every five years, stating:

> 117. (1) After the expiration of not more than 5 years after the coming into force of this Act or part of it and every 5 years thereafter, the minister responsible for this Act shall refer it to a committee for the purpose of undertaking a comprehensive review of the provisions and operation of this Act or part of it.
>
> (2) The committee shall review the list of provisions in Schedule A to determine the necessity for their continued inclusion in Schedule A.

ATIPPA, 2015 came into force on June 1, 2015; June 2025 was the date when the next statutorily mandated review was due to begin. OIPC is hopeful that the Minister of Justice and Public Safety will announce the next review soon.

ATIPPA, 2015 Privacy Breach Statistics January 1 – March 31, 2026

During the first quarter of 2026 (January 1 – March 31, 2026), OIPC received 46 privacy breach reports from 22 public bodies under ATIPPA, 2015. This is a decrease from the 56 breaches reported during the previous quarter.

Public bodies are reminded that OIPC will only be accepting privacy breach reports that are sent using the official OIPC Privacy Breach Reporting Form. All other reporting forms will be rejected, and the public body will need to re-submit. Additionally, public bodies are reminded that personal information should not be included in the breach reports submitted to this Office.

As well, please ensure your breach notification letters to impacted individuals reflect our new physical address: 5th Floor, Beothuck Building, 20 Crosbie Place, St. John's NL. Our mailing address remains the same: PO Box 13004, Station A, St. John's, NL, A1B 3V8.

Summary by Public Body	
City of St. John's	1
College of the North Atlantic	4
Department of Education and Early Childhood Development	9
Department of Forestry, Agriculture and Lands	1
Department of Government Services	9
Department of Health and Community Services	1
Department of Justice and Public Safety	1
Department of Municipal and Community Affairs	1
Department of Social Supports and Well-Being	1
Department of Transportation and Infrastructure	2
House of Assembly	1
Legal Aid NL	1
Memorial University	4
Newfoundland and Labrador Housing Corporation	2
NL Health Services	1
Office of the Child and Youth Advocate	1
Provincial Information and Library Resources Board	1
Town of Main Brook	1
Town of Portugal Cove-St. Philip's	1
Town of Sandy Cove	1
Town of Torbay	1
Treasury Board Secretariat	1