ABOVE BOARD

A QUARTERLY NEWSLETTER BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 09, ISSUE 02 APRIL 2017

CONTACT INFORMATION

Office of the Information and Privacy Commissioner
3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
Email: commissioner@oipc.nl.ca
www.oipc.nl.ca

"The Commissioner's role is to facilitate the effort of a requestor to seek access to information [...] and is effectively an ombudsman or liaison between the citizen and government in attempting to resolve the request by mediation or otherwise if documents or information known to be existing are being withheld in whole or in part for various reasons"
Justice Harrington, NL CA, NL (Information and Privacy Commissioner) v. NL (Attorney General)

OIPC REMINDERS AND UPDATES

Reminder—Time Extension/Disregard/ Extraordinary Circumstances

The OIPC has guidance pieces on our website about the criteria we apply when public bodies come to us seeking a time extension, approval to disregard a request or for variance of a timeline or procedure due to extraordinary circumstances.

We have heard anecdotally that there is a hesitancy on the part of some coordinators to submit these requests to the OIPC. These sections exist in the *Act* in order to balance the right of access with the operational demands of public bodies.

Coordinators should not be reluctant to use these tools if they feel there is a case that can be made for those options. They are there for a reason.

OIPC Website - Keywords No Longer Needed

The OIPC website is now searchable by free-form text search. Your searches are no longer limited to the pre-set keywords.

This new feature is located under the Reports/Commissioner's Reports and enables users to search all PDF documents contained on the website, not just reports.

We anticipate that this will assist our users in more easily locating pertinent documents and will promote further education on access and privacy matters.

Consideration of requests to reinstate the table of concordance will await feedback to see if it meets those needs. Also—if you have any feedback on our website, please email.

QUICK TIPS FOR MUNICIPAL COUNCILLORS

Custody and Control of Records

The *ATIPPA, 2015* applies to all records in the custody or control of a municipality. The physical location of records is just one of many factors to be considered. If a record relates to a municipal matter and the municipality could reasonably expect to obtain a copy of the record upon request, then the record is considered to be in the control of the municipality.

Designation of a "Head"

The *ATIPPA, 2015* requires municipalities to designate a "head" for the purpose of making decisions under the *Act*. Councillors may not make decisions under the *Act* unless they are designated as the head. In cases where councillors are not the head, they are not entitled to decide the information to be disclosed, nor are they entitled to know the identity of the requestor.

Who are Coordinators and What is Their Role?

A "coordinator" is responsible for responding to requests for information. This person may ask you to search your records to determine if you have anything responsive to a request or may independently search for records. You must turn over all records found in relation to a search to the coordinator for his/her review.

Disclosure of Personal Information

In the course of your duties as councillor, if you are required to access personal information, you must only access the minimum amount necessary and you must only use and/or disclose the information only for the purpose it was shared with you. A disclosure of personal information by you that is not in accordance with the *ATIPPA, 2015* is a privacy breach and may constitute an offence.

The Need for Administrative Safeguards

Personal information held by the municipality must be adequately protected against theft, loss, unauthorized collection, use, disclosure, copying or modification and it must be retained, transferred and disposed of in a secure manner. If you must take personal information outside of your municipal office, it should be properly secured in a locked briefcase, or on an encrypted portable device. You must ensure that any electronic devices issued to you as a councillor are password protected and regularly updated with security software.

Disclosure of Your Personal Information in Relation to Your Role as a Councillor

Some personal information about you may be disclosed under the *ATIPPA, 2015* including your position and functions, your salary, opinions given by you in your role as councillor (unless they are opinions about a person other than the person seeking records), and expenses you incurred while travelling at the expense of the municipality.

Much more detail about how the *ATIPPA, 2015* applies to municipalities can be found in the ATIPPA Guide for Municipalities and the full Tip Sheet can be found on our website.

REASONABLE SEARCH GUIDANCE

The *ATIPPA, 2015* does not require a public body to prove with absolute certainty that records do not exist. Rather, the public body must provide evidence to show that it has made a reasonable effort to identify and locate records responsive to the request.

Complaints that a search was inadequate require more than mere assertions to the contrary. An OIPC Review will ask:

- steps that were taken to identify and locate records;
- where (paper files, databases, emails, off-site storage locations) you searched;
- types of searches conducted (i.e. keyword search of email or database, manual search of paper files, etc.);
- when the search took place;
- who conducted searches; and
- why the public body believes no records exist.

Where employees other than the Coordinator have been asked to search for or gather records, Coordinators should ensure that these people are aware that all potentially responsive records must be turned over to the Coordinator. The Coordinator is in the best position to determine what records are responsive and to perform any necessary redactions. Also, specific written instructions should be provided, and a copy kept by the Coordinator, along with the public body's written policy or practice as to how a search should be carried out.

Where a history of conflict or strained relations exists between the person making the request and an employee who is searching for records, and the request is for personal information, the Coordinator should be present for the search or personally conduct the search.

Employees should be made aware that it is an offence to mislead or to attempt to mislead, or obstruct someone who is performing duties under sections 115(2)(b) and (c) of the *ATIPPA, 2015*. This includes a person acting as Coordinator or under the direction of the Coordinator, and the head of a public body.

Records management issues discovered in the process of conducting a search for records should be addressed as soon as possible as inadequate records management practices will not be accepted as a reasonable explanation for failure to locate responsive records.

The full guidance piece can be found on our website.

RECENT OIPC REPORTS

A-2017-006, A-2017-007, A-2017-008—Central Health and Eastern Health

All three Reports related to third party complaints from personal care homes who had been notified by the public body of their right to complain to the OIPC due to the pending release of information. The Reports found that the burden of proof had not been discharged by the Complainant third parties and were critical of the Health Authorities invoking the notice provisions.

Section 19(5)(a) of the *ATIPPA, 2015* requires that public bodies provide some details that address how they arrived at their conclusions when giving notice to third parties, but in all three cases the public bodies provided limited details. In these Reports we highlighted our revised section 39 guidance and the fact that notice to third parties should only be given when a public body is not certain that section 39 applies but do intend to release the records. These Reports highlighted the public bodies' "inappropriate decision to notify third parties" as they clearly stated they felt section 39 did not apply:

> *It has been made abundantly clear by this Office to this Public Body in guidance documents as well in a previous Report, that where a public body determines that section 39 clearly does not apply, it is not required by the Act to notify any third parties. To do so is a needless and unwarranted frustration of timely access to applicants who have their access to information delayed while the notices to and responses of the third parties are dealt with.*

A-2017-002—City of St. John's

The Applicant requested from the City of St. John's a list of properties with arrears of municipal taxes, water taxes and/or interest exceeding $10,000. The City withheld the information on the basis that it would disclose information gathered for the purpose of collecting a tax as set out in sections 39(2) and 40(4)(d) of the *Access to Information and Protection of Privacy Act, 2015*. With respect to section 39(2), the Commissioner found that section 39(2) applied to part of the record and recommended that the name and address fields continue to be withheld. The Commissioner recommended that the amount of tax arrears and tax years for the amounts owing be disclosed.

A-2017-001—Department of Justice and Public Safety

The Applicant requested from the Department of Justice and Public Safety records relating to his dispute with a government department. The Department located one record but withheld it on the ground of section 30 (solicitor-client privilege). The Applicant filed a complaint with this Office. The Commissioner found that the Department properly applied section 30, including consideration and application of the public interest override, and recommended that the Department continue to withhold the record.

OIPC ACTIVITIES

Presentations Completed

During the last quarter the OIPC had delivered presentations related to the *ATIPPA, 2015* to the ATIPP Community of Practice, NL Housing's Labrador Office, the Internal Auditors Association and the Research and Development Corporation.

While most of this quarter's presentations focused on privacy, we offer training and education on all aspects of the *ATIPPA, 2015*. A list of past presentations are available on our website.

Presentations Upcoming

On May 9 the OIPC will address harassment investigators at the Human Resource Secretariat with a focus on section 33 of the *ATIPPA, 2015* (Workplace Investigations).

We are also speaking at the Saskatchewan Connections Conference on May 10, 2017. Commissioner Molloy will be speaking on *ATIPPA, 2015*, its impact on ATIPP coordinators and our Office. He will also review: recent developments in solicitor-client privilege and third party complaints; the "Sunshine List" decision; and, how the hybrid model has impacted the ATIPP complaint process.

We have been invited to speak at the Canadian Association for Civilian Oversight of Law Enforcement Conference on May 30, 2017. The Commissioner will sit on a panel entitled "Transparency in the Disciplinary Process: Ensuring Openness While Respecting Privacy".

Shred for Wishes Event—May 6, 2017

The OIPC is supporting the first annual "Shred for Wishes" shredding event in support of the Children's Wish Foundation. The event will take place from 10 am to 2 pm at 14 Austin Street in St. John's and will be held rain or shine. Protect your own privacy and help children in challenging circumstances.

Outreach Efforts

The OIPC continually seeks opportunities to provide education, training and/or information sessions to community groups, public bodies, professional associations, schools and other interested groups. There is no cost involved.

If you are interested in a session with us please email.

USE OF PERSONAL EMAIL ACCOUNTS FOR PUBLIC BUSINESS

The *ATIPPA, 2015* applies to any records officers and employees of public bodies create or receive in the course of their duties and relate to the business of the public body. This includes those created or received on personal email accounts, although public bodies should **NOT** allow the use of personal email accounts for work. The Office of the Chief Information Officer ("OCIO") has issued a directive with respect to the use of non-government email for work purposes.

ATIPPA, 2015 applies to all records in the custody or control of a public body. The Supreme Court of Canada, in *Canada (Information Commissioner) v. Canada (Minister of Defence)*, 2011 SCC 25, stated that where a record is not in the physical possession of a government institution, it will still be under its control if two questions are answered in the affirmative:

> Do the contents of the document relate to a departmental matter?
> Could the government institution reasonably expect to obtain a copy of the document upon request?

As a general rule, any email that an officer or employee sends or receives as part of his or her work-related duties will be a record under the public body's control, even if a personal account is used.

The Government of Newfoundland and Labrador Email Guidelines provide guidance as to whether an email constitutes a "government record". The Guidelines state:

> *Email constitutes government records if they contain messages created, sent or received by a department that are required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities that document Government of Newfoundland and Labrador business.* [...]
>
> [...] *It is illegal to destroy government records without authorization of the Government Records Committee, as established by The Management of Information Act.* [...]
>
> [...] *When an e-mail is a government record, it is subject to legislation such as the Management of Information Act, the Rooms Act, and the Access to Information and Protection of Privacy Act, and to legal processes such as discovery and subpoena.*[...]

None of these policies reference any distinction whatsoever between records which reside on a government email system versus those which reside on a personal email account.

(CONTINUED OVER)

USE OF PERSONAL EMAIL ACCOUNTS FOR PUBLIC BUSINESS

Officers and employees should also be aware of the obligation contained in section 64 of the *ATIPPA, 2015* requiring that information be protected from theft, loss, unauthorized collection, use or disclosure, unauthorized copying or modification and also retained, transferred and disposed of in a secure manner. A personal email account, which is often web-based, is much less likely to meet these requirements and may allow third-party access to content by not applying adequate security features. Any public body that allows use of personal email accounts to send or receive personal information is therefore risking non-compliance with *ATIPPA, 2015*.

Additionally, the use of personal email accounts does not relieve public bodies of their duty to thoroughly search for requested records and to produce them. Public bodies should be mindful of the challenges that will be presented in identifying and locating responsive records contained in personal email accounts. To address this risk, public bodies should create a policy limiting the use of personal email accounts for work purposes. Acceptance of such a policy should be a condition of employment.

The full guidance piece can be found on the OIPC website.

COMMENDATION—ADVANCED EDUCATION, SKILLS AND LABOUR

During a legislative review, we discovered a Bill to amend the *Income and Employment Support Act* and the *Student Financial Assistance Act*. The new procedure authorized by the Bill would involve staff from two public bodies (AESL and the Student Loan Corporation) being able to access information in a database belonging to the other public body.

As a result of consultation with our Office about how to implement the new program in a manner that addressed privacy concerns, we recommended an Information Sharing Agreement and other future actions (including regular training and software that could accommodate role-based access and audit).

As a result AESL implemented a Systems Use Agreement, which outlines the appropriate and acceptable collection, access, use and/or disclosure of information by staff. This ensures staff are fully aware of, and acknowledge their role in, the protection of personal information contained within all of the Department's computer systems.

The Department consulted with us at every step along the way, and it is a textbook case of how a cooperative relationship between our Office and a public body can yield positive results.

ATIPPA PRIVACY BREACH STATISTICS Jan 1–March 31, 2017

In our most recent reporting period (January 1 – March 31, 2017), the OIPC received 43 privacy breach reports from 18 public bodies under the *ATIPPA, 2015*. This is down from the 52 reports from 21 public bodies received in the third quarter of 2016/2017.

If any public body would like the OIPC to deliver training regarding privacy breaches, or any other topic relating to access or privacy, contact our Office to arrange a time.

Summary by Public Body	
Advanced Education, Skills and Labour	4
Central Health Integrated Health Authority	2
City of Mount Pearl	1
College of the North Atlantic	1
Department of Business, Tourism, Culture and Rural Development	1
Department of Children, Seniors and Social Development	5
Department of Finance	1
Department of Justice and Public Safety	1
Department of Municipal and Intergovernmental Affairs	1
Eastern Health	1
Human Resource Secretariat	1
Memorial University of Newfoundland	1
Newfoundland and Labrador English School District	2
Newfoundland and Labrador Housing Corporation	2
Newfoundland and Labrador Legal Aid Commission	2
Provincial Information and Library Resources Board	1
Service NL	9
Workplace NL	7

Summary by Type	
Email	9
Fax	3
In Person	8
Intentional (i.e. willful breach)	1
Mail Out	11
Other	8
Technical Malfunction	1
Telephone	2

The OIPC issued a tip sheet on Avoiding Inadvertent Privacy Breaches (it can be found on our website oipc.nl.ca)