

QUICK TIPS: For Municipal Councillors

- ① The Access to Information and Protection of Privacy Act, 2015 (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 consider in assessing custody and control. Records not physically on municipal property or in its IT network can still be accessed under the ATIPPA, 2015 if they are in the control of the municipality. Records are considered to be in the control of a municipality if the contents of the records relate to a municipal matter and the municipality could reasonably expect to obtain a copy of the records upon request. See [Canada \(Information Commissioner\) v. Canada \(Minister of Defence\), 2011 SCC 25](#) for further discussion with respect to this issue.

This includes all emails sent on a municipally “owned” email system and also any records created or stored on personal devices or in personal email systems that relate to municipal business. In order for the municipality to remain accountable and transparent, the municipality must have access to all its records, regardless of where they are stored.

- ② The ATIPPA, 2015 requires municipalities to designate a “head” of the municipality for the purpose of making decisions under the Act. This can be one person or a group of people. If councillors are not designated as the head (either individually or as a group), they have no authority to make decisions for the municipality under the ATIPPA, 2015, including decisions about what information can be disclosed to a person that has made a request. They are also not entitled to ask or be advised as to the identity of the applicant making an access to information request.

The OIPC recommends that a permanent employee of the Town be designated as the head in order to avoid any apprehension of bias and to depoliticize the process of answering access to information requests.

- ③ In addition to the head, the municipality also has a “coordinator” who 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 the records, including email accounts. If you are asked to conduct a search, all records found must be turned over to the coordinator so s/he can review them to determine whether they can be disclosed in full or whether redactions should be made prior to disclosure. The identity of the requestor is known only to the coordinator and must remain confidential, often even after the request has been fulfilled.

- ④ In the course of your duties as councillor, you may require access to the personal information of employees, residents or other councillors. In keeping with the privacy provisions of the *ATIPPA, 2015*, the personal information that is disclosed to you must be the minimum amount necessary (unless, of course, the person whom the information is about has consented to the disclosure). Similarly, you have a duty to use and/or disclose the personal information only for the purpose it was shared with you, and again it should be the minimum amount necessary. 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 pursuant to section 115 of the Act. The municipality’s coordinator may be able to help you determine what an appropriate disclosure is or you can also contact the Office of the Information and Privacy Commissioner (OIPC) (see below for contact information).

- ⑤ Personal information held by the municipality must be adequately protected. The *ATIPPA, 2015* requires that municipalities take reasonable safeguards to protect the personal information in its custody and control against theft, loss, unauthorized collection, use, and disclosure, unauthorized copying or modification and to ensure that it is retained, transferred and disposed of in a secure manner. What is reasonable will depend on several factors including the sensitivity of the personal information and the cost of the safeguards. If personal information must leave the municipal offices, it should be properly secured in a locked briefcase (for paper files), or on an encrypted portable device. Never leave records containing personal information in vehicles or otherwise unsecured when you leave your office. Laptops and other electronic devices issued to councillors should be password

protected and regularly updated with security software. Adding personal software and other non-work related applications to electronic devices should be prohibited.

- 6 Some personal information about you may be disclosed under the *ATIPPA, 2015*. This information includes your position and functions as a councillor, 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](#).

You can also contact the OIPC with any questions:

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
Email: commissioner@oipc.nl.ca



www.oipc.nl.ca
1.877.729.6309