Instant Messaging and Personal Email Accounts:

Meeting Your Access and Privacy Obligations

September 2016

Office of the Information and Privacy Commissioner for Nova Scotia

ACKNOWLEDGEMENTS

The Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) gratefully acknowledges that this guidance document is based on the work of the Office of the Information and Privacy Commissioner for Ontario, available on its website at: https://www.ipc.on.ca/resource/instant-messaging-and-personal-email-accounts-meeting-your-access-and-privacy-obligations/ and the Office of the Information and Privacy Commissioner for British Columbia, available on its website at: https://www.oipc.bc.ca/guidance-documents/1515.

CONTENTS

INTRODUCTION

Staff of public bodies and municipalities subject to the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) or the *Municipal Government Act* (*MGA*) have access to a wide variety of popular communications tools and services. Some employees of municipal and provincial government bodies, elected officials and political staff conduct business using instant messaging tools and personal or political party email accounts in addition to their public body-issued email accounts.

These instant messaging tools and personal email accounts create a number of record keeping and compliance challenges. Some of those challenges include:
- searching for and producing records that are responsive to access requests,
- ensuring that records are retained and preserved according to the requirements set out in *FOIPOP* and the *MGA*, and
- ensuring the privacy and security of personal information.

> Records relating to the conduct of a public body's or municipality's business are subject to the access and privacy provisions of *FOIPOP* and the *MGA*, even if they are created, sent or received through instant messaging tools or personal email accounts.

The guidelines below are designed to help you meet your administrative and legal obligations under the Acts.

WHAT ARE INSTANT MESSAGING TOOLS?

Instant messaging tools allow electronic, written messages to be shared in real-time. A few examples of instant messaging tools include:
- Short Message Service (SMS) or Multimedia Message Service (MMS) text messages,
- BlackBerry Messenger (including Personal Identification Number protocol or "PIN-to-PIN" communications),
- internal instant messaging systems, such as Lync,
- online instant messaging applications like WhatsApp, Facebook Messenger or Google Hangouts, and
- any other similar application that allows for real-time, written communication.

ARE INSTANT MESSAGES AND EMAILS SENT FROM OR RECEIVED IN PERSONAL EMAIL ACCOUNTS "RECORDS"?

Yes. The term "record" is defined in section 3(1)(k) of *FOIPOP* and section 461(h) of the *MGA*, in part, as follows: record includes anything on which information is recorded or stored by graphic, electronic, mechanical or other means.

Instant messages and emails are forms of electronic correspondence and are considered records under the Acts, regardless of the tool or service used to create them.

ARE INSTANT MESSAGES AND EMAILS SENT FROM OR RECEIVED IN PERSONAL EMAIL ACCOUNTS SUBJECT TO THE ACTS?

Yes, sometimes. Section 5 of *FOIPOP* and section 465 of the *MGA* state that a person has a right of access to any record in the custody or under the control of a public body or municipality unless specific exemptions apply. The criteria that are used to decide if a record is in the custody or control of a public body or municipality go beyond the physical location of a record and involve factors such as the purpose of the record, who created it, and whether or not it relates to the public body's or municipality's mandate or functions.

A record does not need to be both in the custody and control of a public body or municipality, but rather one or the other. Therefore, in those cases where a record is not in the custody of the public body or municipality, the question is whether it is under the public body's or municipality's control. In deciding this, the OIPC will consider all aspects of the creation, use and maintenance of the information. We will ask questions like:

1. Do the contents of the record relate to the public body's or municipality's business or mandate?
2. Could the public body or municipality reasonably expect to obtain a copy of the record on request?
3. Does the public body or municipality have a right of possession of the record?
4. Does the public body or municipality have the authority to regulate the record's use and disposition?
5. Has the public body or municipality relied upon the record to a substantial extent?
6. Is the record integrated with other records held by the public body or municipality?

Applying this approach, emails sent from or received in personal email accounts may be found to be under a public body's or municipality's control for *FOIPOP* and *MGA* purposes.

HOW CAN YOU MEET YOUR ACCESS AND PRIVACY OBLIGATIONS?

The OIPC strongly recommends that public bodies and municipalities prohibit their staff from using instant messaging tools and personal email accounts for doing business, unless they can be set up to retain and store records automatically.[1]

However, there may be situations where a public body or municipality has a legitimate business need to use these tools or accounts. If your pubic body or municipality is considering using instant messaging tools or permitting the use of personal email accounts, the following steps can help you plan for compliance with the Acts.

ASSESS THE RISKS AND BENEFITS

Conduct a needs analysis to determine when the use of these tools would be appropriate or necessary, and whether the benefits outweigh the risks. This does not need to be a formal review or audit.

Public bodies and municipalities have an obligation to make every reasonable effort to assist applicants who make access to information requests under *FOIPOP* or the *MGA*.[2] This includes a duty to perform an adequate search for records that respond to an access request. The use of personal email accounts or text messages does not relieve public bodies or municipalities of their duty to comprehensively search for requested records and to produce them. While nothing in *FOIPOP* or the *MGA* directly prohibits public body or municipality employees from using personal email accounts or text messages, doing so may make it more difficult for their employer to search for records and so may place them in violation of Nova Scotia's access laws.

In addition, use of personal email accounts and text messages may introduce security risks. *FOIPOP* and the *MGA* require that public bodies and municipalities take reasonable security measures to guard against unauthorized access, collection, use, disclosure or disposal of personal information. Personal email accounts and text message services are often web-based and so much less likely to comply with this requirement than a public body's or municipality's email system.

Another consideration is that Nova Scotia laws require that personal information must be stored only in Canada and accessed only in Canada unless authorized. If an employee is

---

[1] This is consistent with the recommendations made by the Information and Privacy Commissioner for Ontario, the Information Commissioner of Canada and the Information and Privacy Commissioner for British Columbia: Information and Privacy Commissioner for Ontario, "Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations," June 2016, Information Commissioner of Canada, "Access to Information at Risk from Instant Messaging," November 2013, and Office of the Information and Privacy Commissioner for British Columbia, "Use of Personal Email Accounts for Public Business," March 2013.

[2] Section 7(1) of *FOIPOP* and section 467(1) of the *MGA* require public bodies and municipalities to make every reasonable effort to assist the applicant and to respond without delay to the applicant openly, accurately and completely.

using personal email accounts the public body or municipality does not have proper control over the storage and access to that information.[3]

In some cases, there may be a legitimate business need to use instant messaging. For example, university staff may determine that they need to use instant messaging tools to communicate with students.

If it is necessary to use instant messaging tools or personal email accounts for business purposes, do a thorough review of the privacy, security and access implications. The OIPC has a number of privacy impact assessment templates available on our website that can assist you with your review.[4]

Consult with your information technology staff, and records and information management staff to:

- determine the types of tools that best support your public body's or municipality's communications and records management needs.
- determine if records can be automatically and securely retained on your public body's or municipality's digital storage.
- ensure that the tools include search and retrieval functions to support your access to information and other obligations.
- disable unauthorized software on work issued mobile and other computing devices if you can.
- ensure that the records produced by all authorized communications tools are included in your overarching records management plans and training.
- include records created through all authorized communications tools in retention schedules and general records management planning.

> If possible, all communications should be automatically and securely retained on your public body's or municipality's digital storage. Ensure that you can search and retrieve records so that you can meet your access to information and other obligations.

DEVELOP AND IMPLEMENT CLEAR POLICIES

You must develop clear and consistent policies on the appropriate use of communications tools. These policies should:

- identify which instant messaging tools and email accounts are permitted for business-related communications, and clearly prohibit the use of other tools and accounts.
- require staff, if they have sent or received business-related communications using unauthorized tools or accounts to immediately, or within a reasonable time, copy records to their official or authorized email account or to the public body's or municipality's computer or network. This can be as simple as saving a copy to a shared drive or forwarding it to an institutional email account.

---

[3] Section 5(1) of the *Personal Information International Disclosure Protection Act* states that a public body, including a municipality and its service providers, shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada unless otherwise authorized under the Act.

[4] Privacy impact assessment templates are available at: https://oipc.novascotia.ca.

• inform staff that all business-related communications are subject to disclosure and retention requirements, regardless of the tool, account or device used, and that they will have to provide a copy of all business-related communications upon request.
• remind staff that when they are collecting records in response to an access to information request, they must search for and produce any relevant records from instant messaging and personal email accounts.

However you configure your communications tools, staff need clear guidance and training to ensure records are captured and well managed.

Remember that it is not enough to develop policies. Your public body or municipality must ensure that they are implemented. You can do this by developing clear practice and procedure guides and by providing ongoing staff training.

If you think staff are not complying with your policies, you must take immediate action to preserve the records.

While it is not possible to account for every potential situation that may result in non-compliance, clear policies, training and awareness go a long way in encouraging staff to responsibly manage their records. Strong policies also help public bodies and municipalities deal with issues as they arise. In some situations, your public body or municipality may be required to demonstrate that it has made its best efforts to appropriately manage its records. Policies, procedures and guidelines addressing the use of instant messaging and personal email accounts can help do this.

MONITOR AND REVIEW

Your implementation plan should address compliance over time and should include long-term monitoring and review:
• assign someone to answer questions or concerns about your policies, procedures and practices.
• include spot-checks, surveys of staff practices, or other reviews in your plans to ensure that records are being appropriately saved.
• if you think staff are not complying with your policies, take immediate action to preserve the records and prevent further loss of information.

CONCLUSION

Records relating to your public body's or municipality's business that are created, sent or received through instant messaging tools or personal email accounts are subject to the privacy and access provisions of *FOIPOP* and the *MGA*. The use of these tools creates significant challenges for compliance with the Acts and recordkeeping requirements. The OIPC recommends that all public bodies and municipalities prohibit the use of instant messaging tools or personal email accounts when conducting public body or municipality business unless they can be set up to retain and store records automatically. If it is necessary to use these tools, public bodies and municipalities must plan for compliance by implementing appropriate policy and technical mitigation strategies.

CONTACT

Office of the Information and Privacy Commissioner
509 – 5670 Spring Garden Road
Halifax, NS B3J 1H6

Phone:	902-424-4684
Toll Free (NS):	1-866-243-1564
Fax:	902-424-8303
Website:	https://oipc.novascotia.ca
Email:	oipcns@novascotia.ca
Twitter:	@NSInfoPrivacy