Instant Messaging and Personal Email Accounts:
Meeting Your Access and Privacy Obligations

June 2016

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Acknowledgments

The IPC gratefully acknowledges the contributions of staff at Ontario's Ministry of Government and Consumer Services, Ryerson University and the City of London, whose suggestions and insights have informed this paper.

CONTENTS

INTRODUCTION

Staff of institutions subject to the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) or the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) have access to a wide variety of popular communications tools and services. Some employees of municipal and provincial government institutions, elected officials and political staff, including elected officials, conduct business using instant messaging tools, and personal or political party email accounts (personal email accounts), in addition to their institution-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 *FIPPA* and *MFIPPA*
- ensuring the privacy and security of personal information

Records relating to the conduct of an institution's business are subject to the access and privacy provisions of *FIPPA* and *MFIPPA*, even if they are created, sent or received through instant messaging tools, or non–institutional 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
- 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 2(1) of *FIPPA* and *MFIPPA*, in part, as follows:

> "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
>
> (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
>
> (b) … any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution

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?

Section 10 of *FIPPA* and section 4 of *MFIPPA* state that "every person has a right of access to a record or a part of a record in the custody or under the control of an institution" unless specific exemptions apply.

The IPC has set criteria that are used to decide if a record is in the custody or control of an institution. These 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 institution's mandate or functions.[1]

A record does not need to be both in the custody and control of an institution, but rather one or the other.[2] Therefore, in those cases where a record is not in the custody of the institution, the question is whether it is under the institution's control. In deciding this, the IPC considers the following:

1. Do the contents of the record relate to the institution's business?
2. Could the institution reasonably expect to obtain a copy of the record on request?

1 **IPC Order MO-3281** (22 January 2016)
2 **IPC Order P-239** (5 September 1991)

Applying this approach, emails sent from or received in personal email accounts have been found to be under an institution's control for *FIPPA* and *MFIPPA* purposes.[3]

HOW CAN YOU MEET YOUR ACCESS AND PRIVACY OBLIGATIONS?

The IPC strongly recommends that institutions 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.[4]

However, there may be situations where an institution has a legitimate business need to use these tools or accounts. If your institution 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.

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 or to conduct independent research.

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.

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

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

- determine the types of tools that best support your institution's communications and records management needs
- determine if records can be automatically and securely retained on your institution's digital storage

3 **IPC Order MO-3281** and **IPC Order MO-3107-F** (30 September 2014)

4 This is consistent with the recommendations made by the Information Commissioner of Canada and the Information and Privacy Commissioner for British Columbia:

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.

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

- ensure that the tools include search and retrieval functions to support your access to information and other obligations
- if you can, disable unauthorized software on work-issued mobile and other computing devices
- 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 communication tools in retention schedules and general records management planning

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 the institution'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
- 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

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

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

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 institutions deal with issues as they arise. In some situations, your institution 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

You cannot evade access to information requests by using instant messaging tools or personal email accounts for business purposes.

CONCLUSION

Records relating to your institution'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 *FIPPA* and *MFIPPA.* The use of these tools creates significant challenges for compliance with the acts and recordkeeping requirements. The IPC recommends that all institutions prohibit the use of instant messaging tools or personal email accounts when conducting institutional business. If it is necessary to use these tools, institutions must plan for compliance by implementing appropriate policy and technical mitigation strategies.

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three Acts, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction,**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations,**
- **Conducts research into access and privacy issues,**
- **Comments on proposed government legislation and programs and**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Website: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

June 2016