Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools

A Guide for Public Bodies

Considerations for public bodies when using personal email accounts, text messaging and other instant messaging tools for official business to ensure access and privacy obligations are met.

May 2018

Office of the
Saskatchewan Information
and Privacy Commissioner

Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools

A Guide for Public Bodies

Public bodies subject to have access to a wide variety of popular communication tools and services. Some employees of these public bodies conduct business using text messaging and other instant messaging tools.

Public bodies and its employees should **never** use personal or political party email accounts to conduct the public body's business.

Text messaging and other instant messaging tools 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 proper records management practices
- Ensuring the privacy and security of personal information

The guidelines below are designed to help a public body meet its administrative and legal obligations under *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

WHAT ARE INSTANT MESSAGING TOOLS?

Instant messaging tools allow electronic messages to be shared in real-time. A few examples of instant messaging tools include:

- Short Messages 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

Are text messages, other instant messages and emails considered to be "records"?

Yes. The term "record" is defined at subsection 2(1)(i) of FOIP and subsection 2(1)(j) of LA FOIP as follows:

> "record" means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms that produce records;

Emails, text messages and other instant messages 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 5 of both FOIP and LA FOIP provides that "every person has a right to and, on an application made in accordance with this Part, shall be permitted access to records that are in the possession or under the control" of a public body unless specific exemptions apply.

The Information and Privacy Commissioner (IPC) has set criteria that are used to decide if a record is in the possession or control of a public body. 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 public body's mandate or functions.

A record does not need to be both in the possession or control of a public body, but rather one or the other. 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 document relate to the public body's business?
2. Can the public body reasonably expect to obtain a copy of the document upon request?

While our office is of the opinion that official public body business should never be conducted through personal email accounts if emails of a business nature are sent through these personal accounts, those emails would be considered a record pursuant to FOIP and LA FOIP.

How can you meet your access and privacy obligations?

The IPC strongly recommends that public bodies prohibit their staff from texting or using other instant messaging tools for doing business, unless they can be set up to retain and store records automatically.

However, there may be situations where a public body has a legitimate business need to use these text messaging and other instant messaging tools. If an institution is considering using text messaging or other instant messaging tools, it should consider the advice in this resource to ensure compliance with FOIP or LA FOIP.

Assess the Risks and Benefits

Conduct a privacy impact assessment (PIA) to determine when the use of these tools would be appropriate or necessary, and whether the benefits outweigh the risks.

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 text messaging or other instant messaging tools for business purposes, do a thorough review of the privacy, security and access implications.

Consult with access and privacy staff, information technology staff, and records and information management staff to:

- determine the types of tools that best support the public body's communications and records management needs;
- determine if records can be automatically and securely retained on the public body's digital storage;
- determine what format records are saved in and determine if additional software will be required to ensure the public body is able to access the records in a readable format;
- determine where records are stored (i.e. will the information be stored on servers outside of Canada) and ensure that the public body will have control over how that information is protected, disclosed or accessed;
- ensure that the tools include search and retrieval functions to support access to information and other obligations;
- disable unauthorized software on work-issued mobile and other computing devices;
- ensure that the records produced by all authorized communications tools are included in the 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

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 public body associated email account or the public body's computer or network. This can be as simple as saving a copy to a shared drive or forwarding it to a public body's email account. After ensuring these records are saved or forwarded to the public body, the public body should ensure copies on the unauthorized tool or account are destroyed;
- 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.

Remember that it is not enough to develop policies. A public body must ensure that they are implemented. This can be done by developing clear practice guidelines and by providing annual 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 public bodies deal with issues as they arise. In some situations, a public body 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 text messaging, other instant messaging tools and personal email accounts can help do this.

Monitor and Review

An implementation plan should address compliance overtime, and should include long-term monitoring and review.

- Assign someone to answer questions or concerns about policies, procedures and practices
- Include spot-checks, surveys of staff practices, or other reviews in the plans to ensure that records are being appropriately saved
- If staff are not complying with policies, take immediate action to preserve the records and prevent further loss of information.

Conclusion

Records relating to the public body's business that are created, sent or received through any communication tool, including text messaging, other instant messaging tools or personal email accounts, are subject to the privacy and access provisions of FOIP and LA FOIP. The use of these tools creates significant challenges for compliance with the acts and records management requirements. The IPC recommends that all public bodies take appropriate steps to ensure the safeguarding of records sent through text messaging and other instant messaging tools and to ensure compliance with FOIP or LA FOIP. If a public body chooses to use these communication tools, it must plan for compliance by implementing appropriate policy and technical mitigation strategies.

The IPC recommends that all public bodies prohibit the use of personal email accounts for conducting official public body business.

Contact Information

If you have any questions or concerns, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC

Acknowledgement

The Saskatchewan Information and Privacy Commissioner would like to acknowledge that this resource is based on the Information and Privacy Commissioner of Ontario resource *Instant Messaging and Personal Email Accounts: Meeting your Access and Privacy Obligations*: https://www.ipc.on.ca/wp-content/uploads/2016/08/Instant-Messaging.pdf.