Best Practices for the Management of Non-Work Related Personal Emails in Work-Issued Email Accounts

A Guide for Public Bodies

Records management best practices for public bodies for the management of non-work related personal emails in work-issued email accounts to assist public bodies in meeting their access and privacy obligations

This document is intended to provide general best practice advice to public bodies on the management of non-work related personal emails in work-issued email accounts to assist public bodies in meeting their access and privacy obligations.

DISCLAIMER
This document is not intended to provide legal advice and is provided for informational use only.

September 2023

Office of the
Saskatchewan Information
and Privacy Commissioner

Best Practices for the Management of Non-Work Related Personal Emails in Work-Issued Email Accounts

A Guide for Public Bodies

The Provincial Archives of Saskatchewan resource, *Email Management Guidelines*, defines non-work related emails as "those that do not pertain to government business; they are sent to you as an individual, rather than as a government employee. Some examples include invitations to office social events or emails sent to or received from family, friends or professional associations to which an individual belongs."

Please note that for the sake of brevity, in this resource, non-work related personal emails will be referred to as "personal emails" and employees' work-issued email accounts will be referred to as "employee email accounts."

These guidelines will focus on best practices for public bodies in managing personal emails. For guidance on the use of personal email accounts, text messages and other instant messaging tools for official public body business, please see our resource, *Best Practices for Managing the Use of Personal Email Accounts, Text Messages and Other Instant Messaging Tools*.

For guidance on what considerations should be taken into account when deciding to communicate through electronic communication (or eCommunication), please see our resource, *eCommunication: Considerations for trustees to protect personal health information when using eCommunication*.

The guidelines below are designed to assist a public body to meet its administrative and legal obligations under FOIP, LA FOIP or HIPA. Some of the guidance that should be provided to employees on the management of personal emails includes:

- Are personal emails sent from and received in employee email accounts subject to *The Freedom of Information and Protection of Privacy Act* (FOIP),*The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) or *The Health Information Protection Act* (HIPA).

- What the public bodies expectations are for the management of personal emails sent or received from employee email accounts.
- How the management of personal emails can assist a public body in their access and privacy obligations.

For more information on FOIP or LA FOIP, please refer to the *Guide to FOIP, Chapter 1: Purposes and Scope of FOIP* and *Guide to LA FOIP, Chapter 1: Purposes and Scope of LA FOIP*

Are Personal Emails Sent From and Received in Employee Email Accounts Subject to FOIP, LA FOIP or HIPA

Employees of public bodies send and receive emails on a variety of subjects that pertain to its official business. Employees may also send or receive emails using their work email account that are not in any way associated with the public body's official business; these would be considered personal emails.

FOIP and LA FOIP apply to any records in the "possession or under the control of a government institution".

Section 5 of 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 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.

As such, emails are considered records for the purposes of FOIP and LA FOIP. However, the emails would also have to be in the possession or under the control of the public body for the Acts to apply.

It is important to note that just because an email contains personal information of the employee, does not mean the email is a non-work related personal email. The determination of whether it is an official record of the public body or not will depend on the subject matter of the email.

Personal information is defined at subsections 24(1) of FOIP and 23(1) of LA FOIP as: "personal information about an identifiable individual that is recorded in any form." These subsections also provide a list of examples of what qualifies as personal information. As this list of examples is non-exhaustive, the following two-part test can be considered when determining if information qualifies as personal information:

1. Is the information about an identifiable individual?
2. Is the information personal in nature?

An example of an email that may contain personal information of an employee, but may not be a personal email, could pertain to concerns about the employee's performance in their job duties or contain the employee's evaluation related to their work as an employee of the public body. These emails could be official public body records related to potential disciplinary action, salary increases related to their performance in their job duties for the public body or other human resource matters.

In Investigation Report 120-2016, a former employee of a public body submitted a privacy breach complaint concerning the collection of their personal information regarding non-work related activities on the public body's computer equipment during work hours. The public body indicated that the collection took place due to concerns with the employee's standard of work performance and productivity. In that case, it was found that collection of the personal information was authorized for the purpose of managing human resources. In this case, if the non-work related activities included personal emails, these emails would become official public body records, as they were collected for the purpose of managing human resources related to the employee's performance of job duties.

Emails containing work product of an employee is not considered to be personal information and any emails containing work product of the employee would not be considered personal emails. In Review Report 108-2019, the Commissioner found that records containing the fact that an individual worked for a certain public body or had a client that was a public body was considered work product. Additionally, a view or opinion of an individual related to the

subject individual's work in the sector of business they are employed in is also considered work product, not personal information.

The email may also contain personal health information pursuant to HIPA and therefore, the access provision in section 5 of FOIP or LA FOIP would not apply. HIPA applies to personal health information in the "custody or under the control of a trustee".

Personal health information is defined in HIPA as:

- Information about the physical or mental health of the individual.
- Information any health service provided to the individual.
- Information about the donation, testing or examination of a party part or bodily substance of the individual.
- Information collected while providing or incidentally to the provision of health services to the individual.

If the record contains personal health information, in order for HIPA to apply, the following things must also exist:

- There must be a trustee involved as defined by subsection 2(1)(t) of HIPA.
- The organization must have custody or control of the personal health information involved.
- There must be personal health information involved as defined by subsection 2(1)(m) of HIPA.

Therefore, HIPA has a similar requirement in which the public body must have custody (possession) or control of the record, but it must also contain personal health information.

Are Personal Emails Under the Possession or Control of the Public Body

Possession or *custody* is a physical possession plus a measure of control of the record. The mere possession of a record is not enough, there must be some right to deal with the records and some responsibility for their care and protection.

Control connotes authority. A record is under the control of a public body when the public body has authority to manage the record including restricting, regulating and administering its use, disclosure or disposition. To determine whether a public body has records under its control, the following two-part test can be applied:

1. Do the contents of the document relate to a public body matter?
2. Can the public body reasonably expect to obtain a copy of the document upon request?

The first question acts as a useful screening device. If the answer is no that ends the inquiry.

It can be confidently predicted that any government employee who works in an office setting will have stored, somewhere in that office, documents that have nothing whatsoever to do with their job, but which are purely personal in nature. Such documents can range from the most intimately personal documents (such as medical records) to the most mundane (such as a list of household chores). It cannot be suggested that employees of an institution governed by FOIP, LA FOIP or HIPA are themselves subject to that legislation in respect of any piece of personal material they happen to have in their offices at any given time. That would clearly not be contemplated as being within the intent and purpose of the Acts.

While the expectation of privacy may be somewhat circumscribed, there is still both a right to and a reasonable expectation of privacy in relation to certain personal information and personal health information contained on or in government owned equipment and accounts.

In Review Report 096-2015 and 097-2015, the Commissioner found that the emails at issue sent and received in employee email accounts were not created as part of the employee's employment duties and related to the employee's personal matters. It was found that the public body did not have control of the emails at issue, nor did they have possession of the record, for the purposes of FOIP.

In Review Report 007-2019, the Commissioner found that any personal emails sent or received from employee email accounts that were on back-up tapes were not in the possession or under the control of the public body for the purposes of FOIP.

Therefore, personal emails that do not pertain to any aspect of the public body's business, would not be records in the possession or under the control of the public body for the

purposes of section 5 of FOIP and LA FOIP, regardless if the emails reside in the employee's email account.

It is important that public bodies ensure employees are trained to understand the difference between these types of emails to ensure official public body records are being retained.

Best Practices in the Management of Personal Emails in Employee Email Accounts

Develop and Implement Clear Records Management Policies or Procedures

Public bodies should have records management policies or procedures in place regarding how to manage its official business records. Often public bodies have policies in place that also allow employees to use their email accounts for incidental personal use. A public body's records management policies or procedures should also provide employees with guidance on the management of personal emails that are sent from or received in employee email accounts. Some considerations when developing and implementing policies or procedures are:

- Define official public body emails and personal emails. Provide examples of the two types of emails and communicate the difference between these records to ensure official records are retained.
- Encourage employees not to include any non-work related information in an email pertaining to official public body business. For example, an employee may have a personal relationship with someone they are communicating with for work purposes and should refrain from including any personal comments in those emails to prevent non-work related personal comments from becoming part of an official record.
- Consider having employees use a different signature line for personal emails or using features available in the public body's email system to categorize emails as personal to easily distinguish personal emails from official public body emails.
- Explain that email accounts are tools used to communicate, not a storage solution for emails, whether the emails are official public body records or personal emails. As discussed in Review Report 007-2019, as a general rule, employees of public bodies should not use employee email accounts to store personal emails. In this report, the

> Commissioner recommended government institutions develop and implement a policy or procedure on the management of emails, including regularly saving emails to appropriate locations and deleting personal or transitory emails on a regular basis.

Develop and Implement a Documented Best Practice for Accessing Personal Emails

In Review Report 007-2019, the Commissioner also stated that, as a best practice, public bodies should consider having a documented practice in place to provide employees with the ability to gain access to any of their personal emails, after their employment with the public body ceases, within a specified period of time (i.e., within 10 – 30 days of employment ceasing). Public bodies should encourage employees that are ceasing their employment, that prior to their employment end date, they ensure any personal emails are dealt with. However, for those employees that do not have the opportunity to do so, this would provide those individuals with an avenue to access them. As well, if public bodies have the appropriate email management policy in place, as discussed above, the number of personal emails remaining in an employee email account at the time of employment ceasing should be minimal.

How can the Proper Management of Personal Emails Assist a Public Body in Meeting Their Access and Privacy Obligations

Access

When a public body receives an access to information request under FOIP or LA FOIP, it should ensure it has a search strategy for what areas or branches or units should be included in its search efforts in order to determine if there are records responsive to the request. Often, requests involve email records and the public body will conduct a search in certain email accounts using specific keywords to identify if any records are responsive.

Having policies in place that instruct employees to regularly delete personal emails from their employee email accounts may assist in the public bodies' search efforts by reducing the amount of emails that would need to be reviewed to determine if they are responsive.

Reducing the amount of emails that would need to be reviewed could reduce search times, and as a result, reduce the amount of fees associated with a request.

Public body employees should also be aware that personal emails stored in employee email accounts are identified when the public body uses those specific key words, the public body may need to review the content to ensure they are in fact not official business records of the public body. Employees can avoid the possibility of having their personal emails reviewed by the public body by regularly deleting personal emails from employee email accounts.

Privacy

Developing and implementing appropriate policies for the management of personal emails and a best practice to provide an avenue to gain access to any personal emails remaining in employee email accounts at the time employment ceases can reduce the risk of a privacy breach occurring. Unnecessarily retaining copies of personal emails of an employee after their employment with the public body has ceased, with no legitimate business purpose, can result in inappropriate use or disclosure of this information. Reduce the likelihood of a privacy breach occurring by ensuring personal emails are not retained in employee email accounts, filing systems or email backups.

Conclusion

Public bodies should ensure it has clear policies or procedures in place for email management, including guidance on the management of personal emails. These policies should instruct employees that emails pertaining to the public body's official business be saved to the appropriate location and personal emails are deleted regularly from employee email accounts. Having appropriate email management policies in place can assist public bodies in complying with access and privacy provisions in FOIP and LA FOIP.

For information on managing electronic records see our blog *Managing Electronic Records*.

Contact Information

If you have any questions or concerns regarding the management of personal emails in employee email accounts, please contact us:

Office of the Saskatchewan Information and Privacy Commissioner
306-787-8350 | toll free 1-877-748-2298
503 – 1801 Hamilton Street | Regina SK S4P 4B4
intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC | Linkedin