OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Use of personal email accounts and messaging apps for public body business

July 2025

Purpose of this document

This document provides information for public bodies on employees' use of personal email and messaging accounts for work purposes and the requirements of British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA). While FIPPA does not explicitly prohibit employees of public bodies from using personal email or messaging accounts, allowing them to use these accounts is incompatible with FIPPA and exposes public bodies to risks.

Application of FIPPA to personal email accounts and messaging apps (s. 3 of FIPPA)

Section 3 of FIPPA states that the Act applies to all records in the custody *or* under the control of a public body. Emails and messages are records under FIPPA.[1]

Custody requires physical possession and a legal right or obligation to the information. A public body cannot have custody of a record if it does not have physical possession of it.[2]

A public body still has control over emails and messages that are not in its custody if the employee created or received them while performing their duties for the public body.[3]

Therefore, FIPPA applies regardless of whether a public body employee uses their personal or work-provided email and messaging accounts. The head of the public body has legal obligations regarding those emails and messages, including protecting them from unauthorized access and other risks, reporting privacy breaches, responding to FOI requests, and adhering to records retention requirements.

Allowing an employee to use a personal email or messaging account for public body business creates risks for a public body. For example, if the employee's email or messaging service deletes the employee's emails or messages, the public body has no recourse because it has no contractual or business relationship with the provider. Some messaging accounts automatically delete messages after a set time or can be configured to do so.

Allowing employees to use personal email and message accounts also creates risks for a public body with respect to privacy breach reporting. As of February 1, 2023, s. 36.3 of FIPPA requires public bodies in British Columbia to notify affected individuals if a privacy breach could reasonably be expected to result in significant harm to the individuals. Public bodies cannot effectively manage this process if they do not have administrative access to all email and messaging accounts that employees use to conduct public body business.

---

[1] Subject to the exclusions listed in s. 3(1)(a) through (k) of FIPPA.

[2] See Order F22-14, [2022] B.C.I.P.C.D. No. 16 at para. 60.

[3] See Order F20-04, [2020] B.C.I.P.C.D. No. 04 at para. 61.

Adequate search (s.6(1) of FIPPA)

FIPPA requires public bodies to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely. This includes a duty to perform an adequate search for records that respond to an access request. A public body must be able to prove that its search efforts have been thorough and comprehensive and that it has explored all reasonable avenues to locate records.[4] The Information and Privacy Commissioner has the authority to compel the production of records in the custody or under the control of a person,[4] including those in personal email and messaging accounts.

The use of personal email and messaging accounts does not relieve public bodies of their duty to search for requested records and to produce them. Employees may be unwilling or unable (if they are no longer working for the public body, for example) to produce records from their personal accounts or to allow access to their accounts by the public body for that purpose. Additionally, a public body risks over-collecting personal information about the employee and about personal associates of the employee if it tries to access an employee's personal accounts, even with the employee's consent. Section 25.1 prohibits a public body from collecting personal information without authority.

Responsible information management

Individuals living in British Columbia expect accountability from public bodies in their actions as well as in their information practices. One way for public bodies to show this accountability is to create an exact record of their actions in a manner that preserves records of enduring value. When employees of public bodies conduct business through their personal accounts, it is easy for them to lose accountability for those records.

Conclusion

FIPPA applies to work-related email and messages sent to or received from the personal accounts of public body employees. This document shows how the use of personal accounts for work purposes presents risks for public bodies under FIPPA. Public bodies should **prohibit** the use of personal email and messaging accounts to conduct public business. They should have a policy prohibiting the use of these accounts for work purposes, and have all employees agree to follow the policy.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

[4] See s. 44(1)(b) of FIPPA.