Practice Bulletin

Use of Personal Email Accounts for Public Body Business

The purpose of this Guideline is to explain the implications under the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) of the use of personal email accounts for work purposes by employees and officers of public bodies. Officers and employees of public bodies should be aware of two important points: the *ATIPPA, 2015* applies to any records they create or receive in the course of their duties which relate to the business of the public body, including those created or received on personal email accounts. Secondly, public bodies should **NOT** allow the use of personal email accounts for work. The Office of the Chief Information Officer ("OCIO") has issued a directive with respect to the use of non-government email for work purposes (http://www.ocio.gov.nl.ca/ocio/im/employees/non_gov_email.html). This directive makes it clear that subject to clearly approved and documented exceptions in limited cases, the use of personal or non-government email accounts to conduct work on behalf of a Public Body is not permitted. In cases where an exception has been made, or an email respecting government business is inadvertently received in a personal email account, there must be clear processes to transfer the email to an approved government storage location and deleted from the personal or non-government email account, including the "sent" mail folder.

It is important to note that even in the absence of a clear directive prohibiting the use of personal email to conduct Public Body business, the *ATIPPA, 2015* applies to all records in the custody or control of a public body, with the exception of those records set out in section 5(1). The term "custody or control" was explored in depth in our Report A-2014-012. In that Report, the Commissioner reviewed the interpretation of that term in other Canadian jurisdictions. While physical possession may be the best indicator of custody, a public body must have some legal right or obligation to the information in its possession, some right to deal with the records or some responsibility for their care and protection before a public body can be said to have "custody".

The Supreme Court of Canada, in *Canada (Information Commissioner) v. Canada (Minister of Defence)*, 2011 SCC 25, stated that where a record is not in the physical possession of a government institution, it will still be under its control if two questions are answered in the affirmative:

1. Do the contents of the document relate to a departmental matter?
2. Could the government institution reasonably expect to obtain a copy of the document upon request?

The facts of each case will determine whether personal emails are under the control of a public body. As a general rule, any email that an officer or employee sends or receives as part of his or her work-related duties will be a record under the public body's control, even if a personal account is used. This standard will be applied to all public bodies, regardless of the existence of a policy or directive prohibiting the use of personal email for conducting Public Body business.

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

For additional information with respect to what the Government of Newfoundland and Labrador considers when determining if an email constitutes a "government record", see the following resources:

Government of Newfoundland and Labrador Email Guidelines

3.1.1 Which email messages are government records?

Email constitutes government records if they contain messages created, sent or received by a department that are required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities that document Government of Newfoundland and Labrador business. ***These must be managed in the same way as government records in other media, such as paper.***

When email messages fit ***any*** *of the following criteria they* ***are*** *government records:*

- *required to maintain business operations (e.g., emails giving instructions about critical operations or policy direction);*
- *initiate, authorize, document, complete or provide evidence of a business transaction(s) (e.g., documenting a final decision on an issue);*
- *protect the rights of citizens and/or the government (e.g., relate to an individual citizen's or group of citizen's relationship with the government – as a client for example);*
- *provide evidence of compliance with accountability or other business requirements (e.g., document adherence to government policy or provide decision-making trails);*
- *have potential business, legal, research or archival value (e.g., document the development of decision, policy or creation of briefing materials);*
- *reflect the position or business of the department or government (e.g., an email to a citizen stating the department's position or policy on a particular issue);*
- *original messages of policies or directives (i.e., not a message on which the recipient is merely one of many people receiving copies) and, when the information does not exist elsewhere (for example, when the recipient is not merely one of many people copied on the message); and*
- *messages related to employee work schedules and assignments (e.g., an email requesting that a staff person work over time).*

3.3 When can I destroy email messages?

It is illegal to destroy government records without authorization of the Government Records Committee, as established by The Management of Information Act. This ensures a proper legal framework around the disposal of government records and facilitates the identification and preservation of archival and historical records.

The Government of Newfoundland and Labrador E-mail Policy

4.1 E-mail as a government record

The Management of Information Act defines a government record as any record "…created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and an abandoned record…"

Thus, e-mail is a government record when it is created or received in connection with the transaction of Government business (e.g. when it records official decisions; communicates decisions about policies, programs and program delivery; contains background information used to develop other Government documents; etc.) Government records may not be destroyed without the authorization of the Government Records Committee, as outlined in the Management of Information Act.

When an e-mail is a government record, it is subject to legislation such as the Management of Information Act, the Rooms Act, and the Access to Information and Protection of Privacy Act, and to legal processes such as discovery and subpoena.

Any information transmitted via e-mail and classed as a government record, shall be treated in the same manner as any other important records, in any medium, received or created by a department. Such records shall be captured into records management systems. As well, electronic messages captured into a records management system are subject to the provisions of the Management of Information Act, and shall be scheduled for disposal or retention, as approved by the Provincial Archives, according to the class of records in which they belong.

The Information Management and Protection Policy, which includes "any electronically produced document and other documentary material regardless of physical form or characteristic" in the definition of record, also states:

5.0 Policy Statement

The Government of Newfoundland and Labrador manages and protects information in accordance with the Management of Information Act (specifically Section 6), the Access to Information and Protection of Privacy Act and through this policy and associated policy instruments such as directives, guidelines and procedures.

Records in all formats must be managed and protected throughout their lifecycle by any employee or contractor who creates or collects the record as part of their responsibility in performing work for Government.

Records and information must be protected from unauthorized access. Physical and technical means must be applied, as appropriate to the level of sensitivity of the information, taking into consideration requirements to preserve confidentiality, support availability and protect the integrity of the information.

Anyone willfully breaching confidentiality of personal information may be subject to penalty under Section 72 of the Access to Information and Protection of Privacy Act and/or consequences under the appropriate personnel policy of Government, up to and including dismissal, depending upon the severity of the breach.

Breaches of confidential information may be subject to consequences under the appropriate personnel policy of Government, up to and including dismissal, depending upon the severity of the breach.

...

6.0 Information Management and Protection Principles

The OCIO is guided by the relevant International Standards Organization (ISO) and Canadian General Standards Board (CGSB) standards for its policy development framework and overall approach. The development of Information Management and Protection policies, directives, standards and guidelines by the OCIO is based upon the following principles:

***Enabling transparency** of decision-making and expenditure through the development of proper information management and protection practices throughout Government operations and systems, and the appropriate training of information management personnel to provide effective service delivery.*

***Enabling legislative compliance** where a requirement to retain records is articulated or where legislative compliance relies upon timely and appropriate access to information resources.*

***Lifecycle management of all information in all formats** during all lifecycle stages from creation (through use and management) to disposal (through destruction, deletion or transfer to The Rooms Provincial Archives for permanent preservation).*

***Providing information authenticity, integrity and security** to protect information holdings from loss, inappropriate access or use, disclosure, alteration, removal or destruction; thereby ensuring confidentiality, integrity, availability and accountability over time.*

***Risk management** through the assurance that security risks are identified, acceptable and that control mechanisms are in place.*

None of these policies reference any distinction whatsoever between records which reside on a government email system versus those which reside on a personal email account. Other public bodies may wish to refer to some of these resources in creating their own records management and email policies, as well as educating staff on what constitutes a public body record.

Further to the important point of information security, section 64 of the *ATIPPA, 2015* sets out a public body's obligation to take reasonable steps to protect the personal information in its custody or control. This includes protection against theft, loss, unauthorized collection, use or disclosure, unauthorized copying or modification and also a duty to ensure this information is retained, transferred and disposed of in a secure manner. A personal email account, which is often web-

based, is much less likely to meet this requirement than a public body's email system. First, the terms of service for personal accounts may allow third-party access to content in a way that is in contravention of *ATIPPA, 2015*. Second, security features for webmail services may not be adequate for *ATIPPA, 2015* purposes. Any public body that allows use of personal email accounts to send or receive personal information is therefore risking non-compliance with *ATIPPA, 2015*.

In terms of fulfilling the access to information requirements of *ATIPPA, 2015*, public bodies are required 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 are responsive to an access request. A public body must be able to demonstrate that its search efforts have been thorough and that it has explored all reasonable avenues to locate records. If a complaint is filed by an applicant in relation to such a request, it should be noted that the Information and Privacy Commissioner has broad authority under section 97 to compel the production of records.

The use of personal email accounts does not relieve public bodies of their duty to thoroughly search for requested records and to produce them, but this practice can create serious challenges. While nothing in the *ATIPPA, 2015* explicitly prohibits public body officers or employees from using personal email accounts, doing so would certainly make it much less likely that records responsive to an access request would be identified and located. Furthermore, even if it is believed that responsive records may exist on a personal email account, officers or employees may be reluctant to produce records from their personal account or to provide access to such an account for that purpose, creating difficulties for any public body attempting to discharge its responsibilities under the *ATIPPA, 2015*.

To address this risk, all public bodies should create a policy on the use of personal email accounts for work purposes. Acceptance of such a policy should be a condition of employment. The best solution is for public bodies to create a policy which requires the use of its own email system for work purposes. There may be rare circumstances where that is truly not practicable (for example, in a small public body which does not have the resources or expertise to require it). In such cases the policy should be that officers and employees must copy any work-related emails they send or receive to an email account belonging to the public body.

Any information practice of a public body such as the use of personal email accounts which could have the effect of seriously frustrating the accountability and transparency purpose of the *ATIPPA, 2015* must be addressed through clear policy and training. It is also important that this message be clearly endorsed by the leadership of each public body.

The public expects accountability from public bodies in their actions as well as their information practices. An important way for public bodies to demonstrate this accountability is to create an accurate record of all business communications in a manner that preserves records in accordance with the *Management of Information Act*. When officers and employees of public bodies conduct business through their personal email accounts, accountability is too easily lost.

The use of personal email for work purposes presents several challenges for public body compliance with *ATIPPA, 2015*. As such, public bodies should not allow the use of personal email accounts to conduct public business and should ensure that a clear policy is in place in this area and that all officers and employees are aware of and comply with this policy.