Guideline

Email Management

Governance

Authority:	Treasury Board

Audience:	All staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the Government of Newfoundland and Labrador, including all departments and other public bodies as defined under the Management of Information Act (hereinafter referred to as "individual").
Compliance Level:	Recommended
Issuing Public Body:	Office of the Chief Information Officer
	Application and Information Management Services Branch
	Information Management Services Division
Original Issue Date:	2011-04-14
Date Last Reviewed:	2021-06-07
OCIO Reference:	DOC15480/2009
Version Number:	3.0

Notice:

The Office of the Chief Information Officer (OCIO) is mindful of creating and delivering accessible materials, in line with the Government of Newfoundland and Labrador's Accessible Communications Policy. New materials created by OCIO align with policy requirements and modifications to existing materials will occur as part of the standard review cycle.

This document is available in alternate format. Please contact OCIO@gov.nl.ca.

Forward questions and/or comments related to this document to IM@gov.nl.ca.

Table of Contents

1.0   Overview

Email is an effective business tool that, when managed correctly, can provide significant value. However, the volume of email that individuals send or receive poses challenges.

When individuals are aware of best practices that promote the effective management including the capture, use, protection, sharing, disposition and retention of email it supports the efficient and appropriate use of email for government business.

This guideline provides individuals with advice on how to manage email and be more proactive in their own information management (IM) responsibilities concerning email.

This Guideline applies to all government departments and other public bodies as defined under the MOIA and issued under the authority of the Information Management and Protection Policy (IM&P) Policy. The IM&P Policy establishes the foundation for development of all IM&P policies, directives, standards, guidelines and procedures by the OCIO and provides the OCIO with a comprehensive approach in addressing IM&P Policy governance.

Guidelines are recommended actions and general approaches that can guide operational behaviors. They are generally a description that clarifies what should be done and how to achieve the objectives set out in policies, directives and standards. Guidelines are not compulsory, although recommended. Incidental revisions, which may be required from time to time as a result of changes in operational requirements, legislation or other policies, will be made in a timely manner as necessary.

2.0   Purpose

This Guideline provides advice for the use and management of email to both individuals and those with responsibility for IM.

Email messages that document government business are considered government records and should be managed as per the Management of Information Act (MOIA), the Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015) and any other organizational compliance requirements specific to a department or other public body. The MOIA does not allow the disposal of government records unless approved by the Government Records Committee or they meet the definition of a transitory record.

Individuals conducting business activities through email on behalf of the Government of Newfoundland and Labrador's departments and other public bodies are responsible for the following:

— creating, using, communicating and sharing email messages according to these guidelines;

— retaining government records, in a recordkeeping format defined by their departments or other public bodies and organized in a way that makes them easily accessible when required;

— removing records of a personal or transitory nature from email systems on a regular and timely basis;

— protecting government records regardless of format from unauthorized disclosure and from inadvertent loss or destruction;

— protecting personal information according to the requirements of the ATIPPA, 2015; and

— validating email addresses of recipients so that information is sent only to the correct and intended recipient(s).

3.0   Definitions and Acronyms

A complete listing of terms are located on the OCIO website - Information Management and Protection (IM&P) Glossary of Terms.

Individual - For the purposes of OCIO IM policy instruments the definition of individual refers to all staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the Government of Newfoundland and Labrador, including all departments and other public bodies as defined under the Management of Information Act.

Government – For the purposes of OCIO IM policy instruments the definition of "government" refers to public bodies as defined under the Management of Information Act (MOIA) and in some cases may be used interchangeably with the term "departments and other public bodies".

Electronic Mail (Email) – An email is defined as messages created, sent and received electronically between computers and other devices. For the purposes of OCIO policy instruments, email is inclusive of all items contained within the email account including, but not limited to: messages, invites and other calendar items, tasks, contacts, posts, notes, all attachments as well as system metadata. 'Email', 'email messages' and 'email items' (as terms) are often used interchangeably within the OCIO's policy instruments.

Public Body – As defined in the MOIA, a public body is:
  i)   a department created under the Executive Council Act or a branch of the executive government of the province,
  ii)   a corporation, the ownership of which, or a majority of shares of which, is vested in the Crown,
  iii) a corporation, commission, board or other body, the majority of the members of which, or the majority of members of the board of directors of which, are appointed under an Act of the province, the Lieutenant-Governor in Council or a minister of the Crown,
  iv) a court established under an Act of the province, and
  v)   the House of Assembly and committees of the House of Assembly. (Source: MOIA)

Record – A correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform,

electronically produced document and other documentary material regardless of physical form or characteristic. (Source: MOIA)

Government Record - A record created by or received by a department or other public body in the conduct of its affairs and includes a Cabinet record, transitory record and an abandoned record. Disposal of a government record must be sanctioned by a records retention and disposal schedule (RRDS) that has been approved by the Government Records Committee (GRC). (Source: MOIA)

Transitory Record - A government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can be securely destroyed when no longer of value without authorization of the Government Records Committee. (Source: MOIA)

The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
ATIPPA, 2015	Access to Information and Protection of Privacy Act, 2015
IM	Information Management
IM&P	Information Management and Protection
IP	Information Protection
MOIA	Management of Information Act
OCIO	Office of the Chief Information Officer

4.0   Recommended Approach

Within the Government of Newfoundland and Labrador, email is a business tool used by departments and other public bodies. All individuals are accountable for using email appropriately and responsibly.

OCIO recommends the following guidance grouped into four categories to support effective email management.

Email Management Best Practices	Identifying Email as Government Records
Identifying Email as Transitory Records	Email Accounts of Individuals Transferring or Leaving the Organization

4.1   Email Management Best Practices

Guidance to keep in mind when managing email include:

a) All information collected or created in the conduct of business for the government is the property of the government, this includes email;

b) Email messages, regardless of location, are the responsibility of the individual and should be managed properly;

c) Email messages cannot be disposed while an ongoing related access request or legal hold is active in a department or other public body.

d) Email messages required for statutory, legal, fiscal, audit, administrative or operational purposes are official government records and should be managed and transferred to a recordkeeping format (e.g., electronic document management system);

e) Where possible an individual's (service recipient and/or their own) personal information should not be stored in the organization's email system;

f) Individuals should be familiar with OCIO's directives "Use of Non-Government Email Accounts for Work Purposes" and "Acceptable Use of the Government Network and/or Information Technology Assets" when conducting work on behalf of a department or other public body;

g) Individuals should regularly identify and dispose of transitory email messages (as defined in the MOIA and the OCIO's Email Management Directive) that no longer have value due to the temporary nature of the information (e.g., collaboration email(s) need only be retained by lead member not the full group);

h) Individuals should limit email containing confidential or private information and ensure these emails are protected - when appropriate, email attachments should be sent in a secure manner (e.g., password protected, hyperlinks);

i) Individuals should manage the contents of their email account regularly using system functionality (such as the conversation clean up tools with many email applications) as well as following organization-issued recordkeeping practices. This will ease the effort required to locate information quickly, reduce the number of duplicate messages in their mailboxes and avoid exceeding their mailbox limit;

j) Individuals should double check email addresses to ensure messages are sent to the correct recipient as well as regularly manage auto-complete suggested recipients that appear in the To, Cc, and Bcc boxes;

k) Individuals should never send their login ID or password in an email message;

l) Individuals should be cautious when opening email attachments from unknown senders;

m) The organization's email system is reserved for official business requirements. Therefore, an individual's use of government-issued email for personal purposes should be limited and only used per departmental or other public body direction. (e.g., children's school contact);

n) Distribution lists used for sending email should be used cautiously and regularly checked for accuracy;

o) Emails should stay on topic/subject. If an email chain changes to an unrelated subject or to an informal/personal nature consider creating an new email and/or using a less formal communication tool such as instant messaging technologies.

p) Email should not be used for distributing personal opinions unrelated to work, for personal gain, or for inappropriate messages; and

q) Email messages should be professional in tone and written with the same care as any other form of government communication.

4.2   Identifying Email as Government Records

Email constitutes a government record if the email contains information (created, sent or received by a department or other public body) to support or document the delivery of programs/services, to carry out operations, to make decisions, or to account for activities that document government's business functions. These email records should be managed the same way as government records in other media formats in accordance with the MOIA.

Examples of email that are considered a government record include, but are not limited to:

— Messages that provide instructions about operations or policy direction;

— Messages that initiate, authorize, document, or provide evidence of a business transaction(s) or decision;

— Messages that document the position of a department or other public body;

— Messages that provide evidence of compliance with accountability or other business requirements;

—— Messages that have legal, research or archival value; or

—— Messages related to individual work schedules and assignments.

4.3 Identifying Email as Transitory

Transitory records are defined in the MOIA as government records of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. The OCIO website contains additional supports to assist individuals in assessing their records.

Email identified as transitory may be disposed of when they are no longer of value, and shall only be disposed of through means which render them unreadable. (e.g., secure shredding for paper records, deleting electronic records)

Employees are encouraged to dispose of transitory records in a timely manner, this facilitates efficient use of resources as storage and management requirements for these records is minimized.

Examples of email records that may be considered transitory include, but are not limited to:

—— Convenience copies of information retained for reference purposes

   o Copy of a report of a government record available in an alternate location and format;

   o Extra copies of meeting agendas and minutes; or

   o Electronic version of a signed document, where it has been determined that the signed version is the record to be kept and managed.

—— Drafts of records

   o Which reflect content that is included in the final version of the record; and

   o Which contain only minor edits to content or formatting changes.

⎯ Supporting information used in the preparation of a subsequent record

o Working papers, notes and research deemed to be inconsequential.

These examples are not intended to be exhaustive. There will always be exceptions where email might normally be transitory but, due to specific circumstances, they are preserved.

Disposing of transitory records does not require authorization of the Government Records Committee (GRC). If in doubt whether to keep or dispose of transitory records, discuss with a manager or your organization's IM staff.

Once a department or other public body receives an access request, all records in the custody and control of the organization are responsive regardless of whether the records has been deemed transitory.

4.4 Email Accounts of Individuals Transferring or Leaving the Organization

Individuals have a responsibility to manage email and determine how best to manage government records contained within their email account prior to leaving their position. This should be completed through consultation with their immediate supervisor and, where required, the division and/or staff responsible for IM within their department or other public body.

Individuals should dispose of transitory records, forward appropriate email messages to their immediate supervisor, or transfer messages to an appropriate recordkeeping format. This practice supports good information management, meaning only valuable and necessary records are managed and retained as legislatively required.

It is recommended that managers:

⎯ encourage departing individuals to review their email messages and run system tools (such as the conversation clean up tools with many email applications) prior to leaving their position;

⎯ communicate with IT support those responsible for IM support within the department or other public body to ensure best practices for account management (i.e., disabling account) are implemented in a timely manner; and

— communicate with those responsible for IM support within the department or other public body to ensure the required information is retained and/or transferred as necessary.

5.0 Roles and Responsibilities

Deputy Minister or Permanent Head or Designate
(Department or other Public Body)

— Enforce this Guideline across their department or public body.

— Support the department or other public body's compliance with MOIA as well as OCIO-issued policies, directives, standards and guidelines, and ensure that proper protocols are in place to properly manage and eventually dispose of email records appropriately.

Executive, Directors, Managers and other staff responsible for IM
(Department or other Public Body)

— Issue direction to individuals on the organization's protocols for email management.

— Ensure that all individuals receive training in both OCIO-issued and organizational policy instruments regarding the management of email.

Management and other supervisory staff
(Department or other Public Body)

— Ensure all individuals within the program or service area of responsibility are aware of this Guideline.

— Ensure that all individuals under their supervision, who have access to the email system, read and understand these guidelines and that email records of departing individuals are retained, filed and accessible to meet legislative, operational, business and accountability requirements.

Individuals

— Adhere to this Guideline and any related legislation, policies, directives or standards outlining email management requirements including the secure disposal of email determined to be transitory records as a regular course of business.

— Transfer email messages that constitute a government record to an appropriate recordkeeping format so that they can be managed according to the requirements set out in the MOIA.

— Regularly manage transitory records.

— Appropriately review, store and transfer records prior to leaving a position.

Office of the Chief Information Officer (OCIO)

As part of OCIO's administration of the Management of Information Act, the OCIO:

— Recommends to Treasury Board policies for adoption.
— Develops, manages, monitors, and communicates IM&P policy instruments and supporting materials to departments and other public bodies.
— Provides direction on IM&P best practices, resource requirements, organizational structure, recordkeeping systems and IM Programs to departments and other public bodies.
— Assists departments and other public bodies to improve their IM&P capacity.
— Provides IM&P advisory, training and awareness services and support to departments and other public bodies.
— Supports IM forums, committees, and other professional practice communities, consisting of IM representatives from departments and other public bodies.
— Manages the Provincial Records Centre (PRC).
— Provides administrative support to the Government Records Committee (GRC).

In addition, the OCIO will:

— Develop, implement and maintain this guideline.
— Provide education and awareness on the management of email.
— Provide an enterprise email service to departments and other public bodies to transmit and store email messages.
— Provide reasonable measures to protect the email system from unauthorized access.

6.0   Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published location.

Management of Information Act
http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Information Management and Protection Policy
https://www.gov.nl.ca/exec/ocio/im/policy-instruments/im-ip-policy/

Access to Information and Protection of Privacy Act, 2015
http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm

Rooms Act
https://assembly.nl.ca/legislation/sr/statutes/r15-1.htm

Directive - Email Management
https://www.gov.nl.ca/exec/ocio/email-management

Directive - Acceptable Use of the Government Network and/or IT Assets
https://www.gov.nl.ca/exec/ocio/im/employees/asset-use/

Directive - Transitory
https://www.gov.nl.ca/exec/ocio/transitory-records

Directive - Use of Non-Government Email Accounts for Work Purposes
https://www.gov.nl.ca/exec/ocio/im/policy-instrumnets/non-government-email-accounts

Directive – Password Management
https://www.gov.nl.ca/exec/ocio/files/publications-policies-directive-password-management.pdf

Standard – Password Management
https://www.gov.nl.ca/exec/ocio/files/publications-policies-directive-password-management.pdf

OCIO Website
https://www.gov.nl.ca/exec/ocio/

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2011-04-14	1.0
2019-08-27	2.0
2021-06-07	3.0