Office of the Chief Information Officer

Directive

Email Management

Governance

Authority:	Treasury Board Approval TBM (to be determined)
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:	Mandatory
Issuing Public Body:	Office of the Chief Information Officer Application and Information Management Services Branch Information Management Services Division
Original Issue Date:	2020-09-09
Date Last Reviewed:	Not Applicable
OCIO Reference:	DOC01713/2020
Version Number:	1.0

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 4
2.0 Purpose 5
3.0 Definitions and Acronyms 6
4.0 Statements 8
5.0 Roles and Responsibilities 10
6.0 Compliance and Enforcement 12
7.0 Supporting Materials and Version History 13

1.0 Overview

Electronic records, like their paper counterparts, need to be recorded, captured in a form, which ensures their authenticity and integrity, and made accessible. Electronic records need to provide the same evidence of business activity and the same level of accountability as paper records. Electronic records must also be able to meet the immediate and future needs of organizations, individuals and society. Email, as part of this group of electronic records, requires proper management through appropriate organizational-level policies and procedures, as well as compliance monitoring.

This Directive applies to all government departments and other public bodies as defined under the Management of Information Act (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.

This Directive includes management of email regardless of method of access and use (i.e., use of email via desktop/laptop/tablet and any wireless mobile devices).

Directives provide an official authoritative instruction or order to the organization supporting an existing policy. Compliance with OCIO issued directives is mandatory. This policy instrument will be reviewed and updated as required. 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 Directive provides the individuals, departments, and other public bodies' with information to address those email which are considered to be "government records" as defined by the MOIA, making them subject to the same management principles as government records contained in other digital or paper formats.

The Directive promotes the effective capture, management, and retention of email, which are government records, in compliance with information management and protection requirements.

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.

Authenticity – An authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent it, and to have been created or sent at the time purported. (Source: ISO 15489: 2016)

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.

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".

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.

Integrity – Integrity demonstrates that the record is complete and has been unaltered. It is necessary that a record be protected against unauthorized alteration. (Source: ISO 15489-1:2016)

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
ATIPP	Access to Information and Protection of Privacy
EDMS	Electronic Document Management System
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 Statements

1. The Principles outlined in the IM&P Policy support the creation, management, retention and the disposition of records as a routine part of business; this includes email.

2. 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.

3. Email when assessed as a transitory record is a low-value government record of temporary usefulness. If the record is determined to have fulfilled its temporary purpose and no longer has value as a government record than it can be securely disposed.

4. Email assessed as a government record (but not a transitory record) cannot be securely destroyed without the authorization of the Government Records Committee (GRC), as outlined in the MOIA.

5. Email is subject to legislation such as the MOIA, the Rooms Act, the Evidence Act and the Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015), and is subject to legal processes such as discovery, subpoena, audit requirements and access to information requests.

6. Information identified as potentially transitory must be routinely assessed and those records determined to be transitory must be securely disposed of in a timely manner. Retention of transitory records when no longer required significantly affects the discovery process required for information requests (e.g., ATIPP request, audit, inquiry, litigation, etc.).

7. Any information transmitted via email and identified as a government record, shall be treated in the same manner as any form of a record received or created by a department or other public body, and must be managed in the organization's electronic document management system or other records repository.

8. Email messages, and/or attachments required as evidence of a department or other public body's business activity (i.e., those that are considered official government records), shall be captured using one of the following options. The appropriate procedure(s) is to be determined by the department or other public body.

    i) Save the email into an Electronic Document Management System (EDMS) designed specifically for the purpose of managing electronic records; or

    ii) Print the message and any applicable attachments to paper and incorporate into the department or other public body's paper recordkeeping system; or

    iii) Save the message and/or its attachment(s) in a directory outside the email system, which is a part of the department or other public body's official recordkeeping system; or

    iv) Transmit the message electronically to a central records repository or other appointed representative for incorporation into the department or other public body's recordkeeping system.

9. Individuals are responsible for managing their own email accounts. In addition to the requirements outlined in this Directive individuals must keep information, including login names and passwords, secure and confidential in order to protect the security, authenticity and integrity of the records.

10. Email sent outside the organization's email system may not be secure. Therefore, users should be cautious about the type of information sent via email. Confidential information should not be sent via email unless appropriate information protection measures (e.g., hyperlinks, secure file transfer, etc.) are implemented; if an exception is required it should be reviewed with those responsible for IM within the organization.

5.0 Roles and Responsibilities

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

- Enforce this Directive across their department or other public body.
- Support their department or other public body's compliance with the MOIA, the IM&P Policy and other policy instruments issued by OCIO, and other relevant organizational IM&P legal and regulatory requirements.

Executive, Director, Manager and other staff responsible for IM (Department or other Public Body)

- Issue direction on the appropriate procedure for managing email within the department or other public body.
- Ensure that all individuals receive training in both OCIO-issued and organizational policy instruments regarding email use and management.

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 Directive and other related policy instruments.
- Provide direction to individuals working on behalf of the department or other public body on email management as per the organization's mandate.
- When an individual is no longer working on behalf of a department or other public body, it is the responsibility of the individual to which they report to ensure the termination of an individual's email account upon departure.

Individuals

- Comply with the MOIA, the IM&P Policy and other policy instruments issued by OCIO, and other relevant organizational IM&P legal and regulatory requirements.
- Adhere to this Directive 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.

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:

- Maintain the Email Management Directive and any associated supporting materials.
- Provide education and awareness on email management.

6.0 Compliance and Enforcement

Mandatory compliance

OCIO directives are mandatory for individuals to follow and dictate uniform ways of operating.

Compliance monitoring

Compliance monitoring of this Directive is the responsibility of the department or other public body.

Penalty for failure to comply

Willful non-compliance with this Directive, or contravention through negligence, may result in disciplinary action, up to and including termination of employment/contract or other disciplinary action as per the policies and procedures established by Treasury Board and contractual agreements. Human Resource Policies can be accessed through the following link:
https://www.gov.nl.ca/exec/hrs/working-with-us/policies/#4d

7.0 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, TBM (to be determined)
https://www.ocio.gov.nl.ca/ocio/im/im_ip_policy.htm

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

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

Guideline – Email Management
https://www.gov.nl.ca/exec/ocio/files/publications-policies-emailguidelines.pdf

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

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
2020-09-09	1.0