Newfoundland Labrador

Document Title:

Government of Newfoundland and Labrador Email Guidelines

Document Type:	**No. Of Pages**
Guidelines	**19**

Scope:

Government of Newfoundland Labrador

Trim #	**Revision # 10**	**Treasury Board Approval (#)**
		TBM2009-298

Supersedes Email Policy previously approved by **TBM 2006-157**

2009-02-03	2009-10-08	2011-10-08	Shelley Smith Office of the Chief Information Officer (OCIO)	Jean Tilley	Secretary
Date Created	**Approval Date**	**Expiry Date**	**Lead Branch - Name** Information Management Branch	**Policy and Planning**	**Treasury Board Approval**

Table of Contents

1.0 Why do we have email guidelines?

Electronic mail (email) is a means of sending messages between computers using electronic networks and includes sending and receiving messages through the use of government's internal email systems as well as sending and receiving messages across the Internet. It is an integral part of doing business today, effectively replacing a large number of telephone calls, memos, and letters.

With the daily use of email throughout government and society at large, users transmit more and more information electronically without the use of paper documents. This requires the use of effective information management practices in the creation, use and management of email messages, including the identification and retention of emails which are official government records as defined in the *Management of Information Act* and the *Rooms Act*.

1.1 Purpose

The Government of Newfoundland and Labrador is committed to delivering services through electronic means. The purpose of these guidelines is to identify the requirements for proper and responsible management and use of email by public employees and contractors working on behalf of Government of Newfoundland and Labrador. The guidelines recognize email as a valuable resource as a communications medium, and as a tool for disseminating departmental information and facilitating decision-making.

1.2 Scope

These guidelines are applicable to all Government of Newfoundland and Labrador employees and individuals contracted to work for it. This includes all executive, management, unionized and non-unionized levels, who are authorized users of Government of Newfoundland and Labrador email systems, as well as anyone authorized to work on behalf of Government of Newfoundland and Labrador, such as contractors and student employees.

All the information collected or created in the conduct of business for the government is the property of Government of Newfoundland and Labrador, including emails sent and received in the conduct of business either as an employee or contractor of Government of Newfoundland and Labrador.

Furthermore, all Information Technology (IT) systems, infrastructure and software provided by Government of Newfoundland and Labrador is the property of Government of Newfoundland and Labrador, and can be monitored as required, by authorized Government of Newfoundland and Labrador employees. These guidelines apply whether the user is using government equipment, his/her own equipment, or equipment belonging to a third party.

2.0 What are the individual's responsibilities?

Information collected or created in the conduct of business by users of the Government of Newfoundland and Labrador email system is the property of the Government of Newfoundland and Labrador. All users are responsible for the following:

- creating, using, communicating and sharing email messages according to these guidelines;
- retaining government records, in the format and media required by the department and organized in a way that makes them accessible to those authorized to view the contents;
- removing records of a personal or transitory nature from email systems on a regular and timely basis;
- protecting all email government records from unauthorized disclosure to third parties and from inadvertent loss or destruction;
- protecting the personal information of public employees and government clients or citizens in government email messages according to the requirements of the Access to Information and Protection of Privacy Act and government policy;
- disposing of email government records according to authorized records retention and disposition schedules;
- ensuring that, particularly when dealing with sensitive information, the email is sent only to the correct recipient(s),
- ensuring the email addresses of recipients are correct;
- verifying that a distribution list is up-to-date and that the recipients for a particular message are authorized to receive the message before sending it to an entire list; and
- not forwarding another user's email message to a discussion group, Listserv™, newsgroup or posting it on an electronic bulletin board without the user's permission.

Managers are responsible to ensure that all users (including contractors, students, temporary help, etc.,) under their supervision, who have access to the departmental email system, read and comply with these guidelines, and that email government records of departing users (either from the department or their operational area) are retained, filed and accessible to meet legislative, departmental business and accountability requirements.

Information systems managers are responsible for providing a means to transmit and store email messages. They are also responsible for ensuring that these email

messages are preserved and protected from destruction or unauthorized access and that email is securely destroyed once authorization has been acquired.

Information Management Branch, Office of the Chief Information Officer, is responsible for ensuring that users are informed about these guidelines, for publishing them on the Government of Newfoundland and Labrador Intranet and for providing expert advice and guidance on the identification, filing, retention protection and disposal of email records.

3.0 Management of email messages

Along with information in other formats, email messages must be managed with consideration for legislative and policy requirements, and the requirements to provide evidence of business activity. A user should ensure that his/her computer is not left unsecured and that he/she does not share his/her password(s) with others.

Email messages which are government records, as defined in the *Management of Information Act*, must be organized and managed to be easily retrievable and disposed of only in accordance with the provisions of Section 5 of the *Act.* It is the responsibility of the department in cooperation with the Office of the Chief Information Office to store, manage, retrieve, preserve, protect, dispose and transfer email records of employees who have left the department.

Email messages that are transitory records may be deleted once this information is no longer required.

3.1 Email government records

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).

3.1.2 Who is responsible to keep email government records?

The originator (creator) of an email is responsible to ensure that official email government records are retained and managed. This requirement also applies for recipients of email messages sent from external sources, where the information contained in the email does not exist elsewhere in the department, and it forms part of the departmental record. In such cases, that externally generated email will become a government record.

When an originator creates an email message for response from one or several recipients, he/she is also responsible to ensure that the original text and all responses that form the complete email government record are retained.

Emails generated to enable collaboration and information sharing within committees, working groups or work teams do not necessarily need to be retained by all members of the group. The best approach in such situations is to have one member of the group be the "keeper of the records". Email can then be saved in a shared drive or some other means which enables it to be retained and shared as required by group members. The same process can be applied to meeting agenda and minutes.

3.1.3 Are email copies considered government records?

Email messages sent internally for administrative or organizational requirements through postmaster, departmental distribution lists and workgroups, are considered duplicate copies. These messages should be deleted once the information is no longer required. The originator is responsible to ensure that the original messages are retained if they constitute government records.

Replies to any of these emails, add to the information and, therefore, may constitute a new record. In such cases, the person who replies is an originator and must determine whether this new message is a government record and needs to be retained.

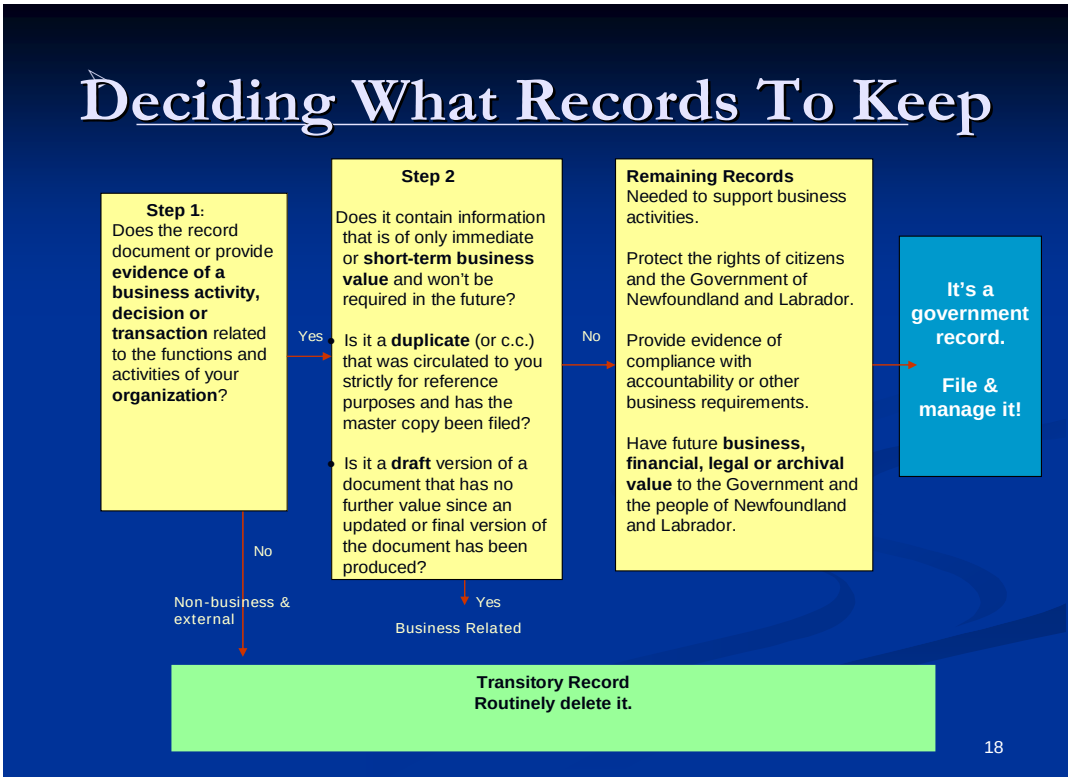
Email messages from sources external to Government of Newfoundland and Labrador, which are distributed solely for information or reference purposes and are not required to

document the business of government, are not government records. These messages should be deleted once the information they contain is no longer required.

3.1.4 Which email messages are transitory records?

Transitory records are records required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record. Email transitory records are not required to control, support or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of the department. The diagram below can help to identify transitory records.

It may be useful to consider that some transitory email may be the sort of information one might share verbally, either in person or by phone, and not feel obliged to follow up in writing.



3.1.5 Backup and retention of email

Back-up measures have been established for Government of Newfoundland and Labrador email systems for disaster recovery purposes. These measures permit information to be restored should the system crash or the email system be damaged in some other way.

These procedures provide emergency back-up for server based mail systems and are **not** an email archive from which users can routinely restore accidentally deleted emails.

3.2 How do I file email?

Key concerns when filing email messages and attachments will be the ability to identify, retrieve and share this information, as required. If a user has established that an email message is a government record it must be managed and retained appropriately.

It is not recommended to keep an email record in more than one format. If it has been printed and filed, the electronic copy should be deleted. If the email has been filed in an Electronic Document Management System (EDMS), such as a TRIM system or shared directory, the copy in the email in-box should be deleted.

3.2.1 What is an Electronic Document Management System (EDMS)?

An Electronic Document Management System (EDMS) captures and stores electronic documents (including email messages) in a central repository. It allows users to assign information about records (metadata), such as a document title, subject, description and access rights. As well, an EDMS also automatically assigns such information as name and organization of the person filing the record, the document application type, etc. Authorized users can then research and retrieve documents based on the metadata entered in the system, or by using full-text searches.

An EDMS provides greater control for the management, identification and retention of an organization's electronic documents. It allows for the life-cycle management of this information in electronic format and facilitates the sharing of this information with broader audiences.

A government-wide initiative is under way to configure TRIM and implement it throughout Government of Newfoundland and Labrador with standard configuration, classification and practices. TRIM, along with the standard classification plan being developed by the Office of the Chief Information Officer will address document naming conventions, version control, authentication, workflow, records classification, security, and records disposition according to approved records retention and disposition schedules. TRIM can also handle the management of paper records with file folder and box level information.

Until TRIM is in place across government, departments and users must use existing technology to manage email records and other electronic records. Each department will have to examine the advantages and disadvantages of each approach for different groups of records and employ the approach which works best in their environment. The Office of the Chief Information Officer can provide advice through its Information Management Branch.

3.2.2 Records offices and hard copy files

In departments where there is no EDMS, it is advisable to print email government records for filing.

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.

3.3.1 When can I get rid of email government records?

As with any departmental record, email records, depending on their individual function and content, have varying retention periods. Retention can range from very short to long term according to the need for the record. Therefore, it is impossible to apply a universal rule to delete all email messages after a set period.

Departmental records can only be disposed of after legal authorization. These authorities include the Government Records Committee approval to dispose of records and the The Rooms, Provincial Archives subsequent decision on the form of disposition (either destroy records or transfer them to the The Rooms, Provincial Archives). While generic disposition authorities exist for administrative records (IMSAR) there is no standard authority for operational records.

Disposition authorities currently used for departmental records can be applied to either paper or email records maintained in electronic format. These authorities specify the approved retention periods. They should be applied only under the guidance of personnel trained in information management.

3.3.2 When can I destroy email transitory records?

Email messages determined to be transitory in nature (for definition of transitory records see section 3.1.4) should be regularly deleted once they are no longer of use to the email creator or recipient.

The only exception is if a department has already received a formal request under the *Access to Information and Protection of Privacy* legislation or is involved in a legal discovery process – **no email should be deleted if it is required for these reasons.**

3.3.3 Deleting email

Empty the “deleted items” folder regularly. Users should do regular clean-ups of their email in-box and “sent items” folder by filing email government records and by deleting the transitory emails. Refer to Section 2, Management of Email Messages. Regular clean-ups will prevent receipt of “mailbox full” messages, and will enable users to find and share information faster.

3.4 Responsibilities of departing/moving employees

Departing employees are responsible for ensuring that their email government records and their mailboxes are in order before their departure. Departing employees must save and file all those messages determined to be government records, as per the Email Policy and the guidelines outlined in this document. One or more of the following options may be employed:

- saving email government records to TRIM (preferred option where TRIM is available);

- filing email government records in electronic format within a shared directory in the appropriate directory files (if using a shared directory);

- with their manager's approval, assigning responsibility for an email account to another person with the understanding that this person will not delete email government records of the departing employee; and

- printing and filing email government records in the applicable records office or other applicable filing area. This would be appropriate in situations of a temporary nature such as maternity leave, secondment, etc.

Departing employees should delete all those messages that are not government records. If an employee is merely transferring within a department or departing for a temporary period of time and retaining his/her current email account, he/she may wish to keep his/her emails.

3.4.1 Managers' Responsibility

Before conducting the clean-up of email messages, a departing employee should consult with his/her supervisor to determine and agree upon the filing method for email government records. Managers are responsible to ensure that email government records, as well as those identified in Section 1.2, remain within the department. They are also responsible for ensuring that these email records are identified and filed so that they can be researched and retrieved, as required.

3.4.2 Removal of email accounts

When an employee is departing; the relevant Human Resources Division will inform the Office of the Chief Information Officer. The Office of the Chief Information Officer will remove the email account from the mail system after receiving confirmation from the departing employee's manager that no government records are stored in the email account. All records retained in the email account will be permanently deleted.

3.4.3 Abandoned Email Disposal Process

The *Management of Information Act* defines an abandoned record as:

> "a government record to which ownership cannot be established and which has been determined to be an abandoned record by the chief information officer.."

A process for disposing of email accounts that contain abandoned records has been designed to accommodate exception to the regular management processes. It is expected that managers will ensure that departing employees will ensure that all government records are appropriately classified and filed in the departmental records management system. The need to manage abandoned email should therefore be limited.

In the event that an email account is abandoned the Office of the Chief Information Officer (cooperation between the IT and IM divisions) will undertake the following steps to facilitate disposal of the records in the account:

- Identify the name(s) on the account;
- Submit the name(s) to the Deputy Minister requesting sign-off for archival appraisal and disposal of records;
- Departments will be required to provide some additional information on the owners of the email boxes including position title, division/branch, and identification of current email filing guidelines (if available) in the Department;
- The Chief Information officer of the Office of the Chief Information Officer will authorize the designation of the email account as abandoned.
- The Rooms Provincial Archives government records archivist will complete a functional macro level appraisal by account;
- Accounts to be destroyed will be submitted to the Government Records Committee for official sign-off and deleted from mail servers;
- Accounts to be archived will be stored on off-line storage for the retention time identified by the Rooms Provincial Archives (actual process to be determined in consultation with the Office of the Chief Information Officer and the Provincial Archives); and

4.0 Creating and using email

4.1 How to use email effectively

Email provides an ideal tool to quickly and easily communicate and share information. It allows users to send information to one or several recipients simultaneously, offering greater opportunities for productivity. Each user is responsible to implement practices to reduce the "clutter" or volume of email traffic on a system including:

4.1.1 Misuse of email

Users can easily fall into the trap of forwarding chain letters or SPAM to other users. These types of messages are frequently hoaxes that entice or may even insist that recipients forward them on. Recipients of an email SPAM or chain letter should not forward or reply to it. Recipients are responsible for this email and should delete it immediately from their mailboxes.

The government has anti SPAM filters in place to try to prevent SPAM from entering the government email system. The process for determining SPAM is not one hundred (100) per cent accurate, what is SPAM or junk mail to one person may be a legitimate piece of mail for another.

To prevent legitimate email from being stopped, the addresses of known legitimate senders can be placed on a "safe" list so that mail from these sources will be delivered. In cases where a user feels her/his legitimate mail may be being caught by SPAM filters, he/she should contact the Office of the Chief Information Officer Helpdesk concerning adding addresses to the exclusion list.

4.2 Who owns email on the Government of Newfoundland and Labrador system?

Email messages created in the conduct of government business are the property of the Government of Newfoundland and Labrador. They may be accessed by government personnel who are authorized to do so and have an appropriate reason for access.

4.3 What legislation applies to email?

Email messages, identified as government records, are subject to the same legislation and policies as other government records. These include, for example: the *Management of Information Act,* the *Rooms*, the *Access to Information and Protection of Privacy Act*, the *Evidence Act, t*he *Electronic Commerce Act* and the discovery of evidence rules in the Rules of Court.

4.4 Legal issues

Email messages may be evidence in legal proceedings. Rules of disclosure are the same as for paper records. This means that organizations can be required to provide their email messages in legal proceedings.

Email must be used in compliance with Canadian and Newfoundland and Labrador laws and regulations. Activities such as disseminating messages that promote hatred against identifiable groups or an individual, distributing obscene material, or violating another person's copyright, are unlawful.

4.5 Can anyone gain access to a user's email?

Email created or received in the conduct of departmental business must be accessible for business-related purposes, and meet legislative and departmental accountability requirements. This underscores the need for the regular maintenance, organization and filing of email government records, and the deletion of non-government record material.

With the exception of email covered by specific exemptions the public can gain access to email messages under the *Access to Information and Protection of Privacy Act*.

4.5.1 Monitoring of email

To mitigate any security concerns, and to ensure that email is not misused, the Government of Newfoundland and Labrador shall monitor email traffic and content for viruses and SPAM, so that problems can be investigated.

The Government of Newfoundland and Labrador scans all email messages that pass through its infrastructure to check for computer viruses, worms or other malicious items that could pose a threat to the security of the Government of Newfoundland and Labrador network. All efforts will be made not to transport questionable email to and from the user. For additional details on email monitoring practices of the Government of Newfoundland and Labrador please contact the Office of the Chief Information Officer Help Desk.

Access to email by system administrators

System Administrators may be required to access email accounts. This will be done only in limited circumstances, such as:

- with a user's permission, to rectify a problem;
- by a Deputy Minister (or delegate), to access a specific business-related email. This would occur in a situation when the user is away from the office or unavailable and where the email is otherwise inaccessible and is required immediately. The user will be notified by Human Resources or her/his Deputy Minister (or delegate) of this action; and
- to investigate suspected misuse of email.

Collection, use and disclosure of personal information of employees, citizens or clients involving an email system will be done in accordance with the legal requirements of the *Access to Information and Protection of Privacy Act* to investigate suspected misuse of email.

4.5.2 Email system audit trails

System audit trails automatically record the circumstances surrounding log-in attempts, creation, transmission and receipt, filing and retrieval, updates and deletion of messages in an email system or on a network. The Government of Newfoundland and Labrador maintains email system audit trails.

4.6 Privacy

Users should seriously consider privacy and confidentiality when choosing email as a means of communication.

Choosing email to communicate personal information about a third party or a user's own personal information, or to send information that is security classified, considerably increases the likelihood of unauthorized disclosure. Email messages could be intercepted in transit or be read by someone else. It is also important for users to remember that email messages can easily be forwarded to others, or even accidentally sent to the wrong address.

4.7 Security

The Government of Newfoundland and Labrador does not currently have enabled security features with the ability to digitally sign and/or encrypt email messages and attachments. Without such protection, information transmitted electronically can be easily compromised by casual eavesdropping at message storage points or by deliberate monitoring of the circuit. A key concern about system integrity is the possibility that an email message may never reach its intended recipient and the sender may be unaware of that fact.

Users should always use email with the assumption that messages may be read by someone other than the intended recipient. Think of email as an electronic postcard. It is not in an envelope and any system that it passes through has the potential ability to read its contents. Users should write email records with the same professional standard they would apply to creating paper records.

By the very nature of the internet, once an email message leaves the Government of Newfoundland and Labrador network, there is no control over what systems it passes through en route to the intended recipient.

4.7.1 Security of Attachments

Attachments are a serious security threat because of their potential for damage. They can automatically scan the user's address book and send an infected message to the addresses. As well, viruses can be attached to any type of file. The majority of users open attachments without question, or even have their software open attachments automatically upon receipt. Users are advised to:

- Avoid opening suspicious attachments, regardless of the sender;
- Check with the sender about the authenticity of an attachment before opening it; and

- Turn off the email function that automatically opens attachments.

5.0 References

5.1 Relevant Legislation

The management of Government information exists within a legislative framework that spans several departments and types of functions and authorities, including individual departments, the Office of the Chief Information Officer, the Provincial Archives, the Government Records Committee, the Office of the Access to Information and Protection of Privacy Coordinator, Information Technology and Information Management Personnel and individual public employees.

Management of Information Act - http://www.hoa.gov.nl.ca/hoa/statutes/m01-01.htm

Rooms Act - http://www.hoa.gov.nl.ca/hoa/statutes/r15-1.htm

Access to Information and Protection of Privacy Act - http://www.hoa.gov.nl.ca/hoa/statutes/a01-1.htm

Transparency and Accountability Act - http://www.hoa.gov.nl.ca/hoa/statutes/t08-1.htm

Evidence Act - *http://www.hoa.gov.nl.ca/HOA/statutes/e16.htm*

Electronic Commerce Act - *http://www.hoa.gov.nl.ca/hoa/statutes/e05-2.htm*

Financial Administration Act - http://www.hoa.gov.nl.ca/hoa/statutes/f08.htm

5.2 Policies

- Blackberry Usage Policy
- IT Security Framework – under development
- Email Policy - http://www.ocio.gov.nl.ca/im/policies/email/email_policy.pdf
- Access to Information and Protection of Privacy Act Policy and Procedures – under development

6.0 Key Contacts

- IM Branch, Office of the Chief Information Officer
    - im@gov.nl.ca
    - 729-0227
- The Rooms Provincial Archives
    - archives@therooms.ca
    - 757-8030
- Office of the ATIPP Coordinator
    - 729-7939
- Office of the Chief Information Officer Help Desk
    - 729-4357 or servicedesk@gov.nl.ca

Appendix 1 – Glossary and Terms

- Abandoned Record
- Active Record
- Administrative Records
- Archival Appraisal
- Authenticity
- Back-up
- Classification Plan (file)
- Data Conversion
- Data Migration
- Destruction
- Disposal
- Disposition
- Electronic Document Management System (EDMS)
- Email
- Encryption
- Government Record
- Government Records Committee (GRC)
- Information Management System for Administrative Records (IMSAR)
- Integrity
- Inventory
- Life Cycle
- Metadata
- Office of Primary Responsibility (OPR)
- Operational Records
- Records Management System
- Records Retention and Disposal Schedule
- Reliability
- Semi-active Records
- SPAM
- Structured Record
- Transitory Record
- TRIM
- Unstructured Record
- Usability
- Vital Record

Abandoned Record - An abandoned record is a government record to which ownership cannot be established and which has been determined to be an abandoned record by the Chief Information Officer (CIO) of the Office of the Chief Information Officer (OCIO).

Active Record - A record which is regularly referenced or required for current use (also called a current record). These records are usually kept within the primary office space or in a records centre or registry.

Administrative Records - Administrative records are required by all organizations to function. These "lights on" records document administrative processes including human resources, general administration, facilities management, financial management, information and information technology management, and equipment and supplies (material) management. Because the value of these records is consistent across Government Departments, the OCIO maintains the Information Management System for Administrative Records (IMSAR) as a standard for their management.

Archival Appraisal - Archival appraisal is the process of determining the long term value of records after they have completed the primary purpose(s) for which they were created. Approximately 95% of all records created have no archival value and should be destroyed at the end of their life cycle.

Authenticity – Authenticity verifies that a record has not been modified or corrupted following creation, receipt, migration or conversion.

Back-up – A Back-up is a copy of a record that is any of the following:

- Additional resource or duplicate copy on different storage media stored offline for emergency purposes
- Disk, tape or other machine readable copy of a data or program file
- Data or program file recorded and stored offline for emergency or archival purposes
- Record that preserves the evidence and information it contains if the original is not available

Classification Plan: A classification plan is the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules and represented in a classification system.

Data Conversion – Process of changing records from one medium to another or from one format to another.

Data Migration – Data Migration is moving sets of recorded information from one Information Technology System or device to another, as required by changes in a system configuration or requested by a user, while assuring that the data will be addressable and that data integrity will be maintained in the new environment.

Destruction - The physical destruction of records that are deemed to have no archival value.

Disposal – Disposal in the context of a records retention schedule, disposal can mean either destruction of records or transfer to archives for permanent retention. It is the final stage of the records life cycle or continuum.

Disposition - In the context of a records retention schedule, disposition can mean either destruction of records or transfer to archives for permanent retention. It is the final stage of the record's life-cycle.

Electronic Document Management System (EDMS): An EDMS is a software package which provides tools for storing and managing unstructured electronic records. TRIM is an example of an EDMS.

Email: Email is defined as messages, including attachments sent and received electronically between personal computers or terminals linked by communications facilities. This includes address information (to, from, cc, bc, subject and date) and the message content.

Encryption – Encryption is the operation by which plain text is modified with an intelligible, non-exploitable text making it non-retrievable except by authorized users that have the key to bring it back to its original form.

Government Record - A Government Record is a 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. Disposal of a government record must be sanctioned by a records retention and disposal schedule that has been approved by the Government Records Committee (GRC).

Government Records Committee (GRC) – the GRC is the official body that is mandated to:

- Review and revise schedules for the retention, disposal, destruction or transfer of government records.
- Make recommendations to the minister respecting public records to be forwarded to The Rooms, Provincial Archives.
- Authorize disposal and destruction standards and guidelines for the lawful disposal and destruction of public records.
- Make recommendations to the minister regarding the removal, disposal and destruction of records.

Information Management System for Administrative Records (IMSAR) – IMSAR is provides a records retention and disposal schedule for administrative records that can be used by all government departments.

Integrity - Integrity demonstrates that the record is complete and has been unaltered.

Inventory – And Inventory is a detailed survey of the organization's records, including descriptions, scope, volume, frequency of use, method of organization and retention periods. It is used as the basis for developing a records management system.

Life Cycle – The life cycle refers to the stages through which information is managed. Information management strives to manage the records in a manner that facilitates authenticity, reliability, integrity and usability throughout all stages including:

- Planning
- Creation and organization
- Receipt and capture of data
- Retrieval, processing, dissemination and distribution of data;
- Storage, maintenance and protection
- Archival preservation or destruction or expungement

Metadata – Metadata is data about data elements including data descriptions, data ownership, etc. Metadata provides the information required to manage records. The creation and end date, for example are key pieces of information required to implement a records retention and disposal schedule.

Office of Primary Responsibility (OPR) – The OPR (also called Office of Record) is the office which creates or acquires the original of a record, and is responsible for maintaining it. Copies of the original which may exist in other offices generally have shorter retention periods than the original in the OPR.

Operational Records - Operational Records are records which are unique to the mandate of their creators. Unlike administrative records, these will be different in each organization. Each Department is responsible for the development, implementation and maintenance of records retention and disposal schedules for the operational records that they generate/receive.

Records Management System: An information system primarily designed to assist an organization in managing its recorded information concerning its recordkeeping practices from inception to disposition of records.

Records Retention and Disposal Schedule: A records retention and disposal schedule is a legal document that guides the management of a government record.

- Define the content of the record series or types.
- Link the records to the organizational unit and business process
- Dictate how long the records need to be retained in active and semi-active storage to meet operational and legislative requirements
- Authorizing the disposition of information in a legal manner.

Reliability – Reliability affirms that the content of a record is a trustworthy and a complete account of an activity or process.

Semi-active Records – Semi-Active records are those records that do not have to be readily available in primary offices but which still need to be kept for the possibility of use or reference. These records should be stored in appropriate storage facilities.

SPAM: Spam refers to electronic junk mail or junk newsgroup postings. It is defined in more general terms as any unsolicited email. In addition to being a nuisance, spam also eats up a lot of network bandwidth.

Structured Records - Structured records are defined as information stored in fields and rows in tables in a relational database. Structured records may constitute a government records when generated or received to complete government business transactions.

Transitory Record - A transitory record is 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 a records retention and disposal schedule.

TRIM: TRIM is the standard electronic document management system (EDMS) of the Government of Newfoundland and Labrador. Information about TRIM can be found at www.towersoft.com/na (LINK), or by contacting the Government of Newfoundland and Labrador TRIM Program Manager at 729-6723.

Usability - Usability refers to the ability to locate, retrieve, present and interpret records over time.

Unstructured Records - Unstructured records are defined as masses of information which do not have a data structure or one that is easily readable. Unstructured records are created via common desktop applications, such as Microsoft Outlook, Word and Excel, etc. to support ongoing business activity. An EDMS like TRIM is used to manage unstructured records.

Vital Record - Records necessary to continue the operation of an organization in case of emergency or disaster.