Northwest Territories

Guideline

6003.00.21

GNWT
INFORMATION TECHNOLOGY
Managing Electronic Mail Messages

1. Statement

Information is a valuable asset that the Government of the Northwest Territories must manage as a public trust on behalf of the residents of the Northwest Territories.

The intent of this guideline is to provide direction to employees of the Government of the Northwest Territories for the effective management of information contained in e-mail messages.

2. Guideline

Employees of the GNWT are encouraged to manage their e-mail messages based on the attached Guidelines on Managing Electronic Mail Messages.

3. Supporting Documentation and Information

a) Policy 6003.00.18 Recorded Information Management
b) Policy 6003.00.20 Management of Electronic Information
c) Attached GNWT Guideline 6003.00.21 on Managing Electronic Mail Messages

4. Implementation

This Guideline applies to all employees of the GNWT as defined in the Public Service Act. It also applies to anyone authorized to work on behalf of the GNWT, such as contractors, students, and temporary help, who have access to the GNWT e-mail system.

Chairman of the Informatics Policy Committee (IPC)

Northwest Territories

Guideline

6003.00.21

GNWT
INFORMATION TECHNOLOGY
Managing Electronic Mail Messages

1. Statement

Information is a valuable asset that the Government of the Northwest Territories must manage as a public trust on behalf of the residents of the Northwest Territories.

The intent of this guideline is to provide direction to employees of the Government of the Northwest Territories for the effective management of information contained in e-mail messages.

2. Guideline

Employees of the GNWT are encouraged to manage their e-mail messages based on the attached Guidelines on Managing Electronic Mail Messages.

3. Supporting Documentation and Information

a) Policy 6003.00.18 Recorded Information Management
b) Policy 6003.00.20 Management of Electronic Information
c) Attached GNWT Guidelines 6003.00.21 on Managing Electronic Mail Messages

4. Implementation

This Guideline applies to all employees of the GNWT as defined in the Public Service Act. It also applies to anyone authorized to work on behalf of the GNWT, such as contractors, students, and temporary help, who have access to the GNWT e-mail system.

Chairman of the Informatics
Policy Committee (IPC)

Table of Contents

1. *Introduction*

Electronic mail (e-mail) is a means of sending messages between computers using electronic networks. It includes sending and receiving messages through the use of e-mail systems as well as sending and receiving messages across the Internet.

E-mail is an efficient and timely communication tool used to conduct business within government, with business partners, and with the public. E-mail can increase productivity, reduce costs, and help improve the way we conduct business. E-mail expedites business communications, reduces paperwork, and automates routine office tasks. The advantages of e-mail have led to a rapid growth in the use of this technology.

The growth of this form of communication underlines the fact that electronic mail messages, like other forms of records, must be managed in accordance with the business needs of the department and Government of the Northwest Territories (GNWT) legislation and policies.

The *NWT Archives Act* and the *Access to Information and Protection of Privacy Act (ATIPP)* include within their definition of a public record, e-mail messages. Therefore, e-mail messages must be managed by the same principles used to manage records in other formats. The key principle is that public records must be managed throughout their life-cycle or, in other words, from the time a record is created or received through to its final disposition.

In the GNWT managing the life-cycle of a record, regardless of its format, is accomplished through the use of the Administrative Records Classification System (ARCS) and the Operational Records Classification System (ORCS).

The following guidelines provide instruction for managing e-mail messages through all the phases of their life-cycle. From creation, distribution and use, through to their final disposition, destruction or transfer to the NWT Archives.

1.1 Purpose

These guidelines recognize e-mail as an ideal tool to quickly, easily, and cost-effectively communicate, share, use, and access information. However, they also identify issues around e-mail use, such as those related to access, privacy and security, and the potential for misuse.

This document requires GNWT employees to apply proven information management practices to e-mail messages. It gives guidance to employees in the creation, use, and management of e-mail messages. It also assists in the identification of those e-mail messages that are public records. Finally, it explains how to dispose of e-mail

messages to make sure that information for which the GNWT is accountable is not lost or inappropriately destroyed.

1.2 Scope

These guidelines apply to all employees of the GNWT as defined in the Public Service Act. They also apply to anyone authorized to work on behalf of the GNWT, such as contractors, students and temporary help, who have access to the GNWT e-mail system.

1.3 Ownership

E-mail messages that employees create in the conduct of GNWT business are public records and belong to the GNWT. They are needed as evidence of business activities, to comply with legislation, and to be accountable to the public. Employees are responsible for making sure that e-mail messages are filed within the department's records classification system. Refer to *section 4, Management of E-mail Messages*, for more detail on identifying and managing e-mail messages.

1.4 Legislation and Policy

E-mail messages are subject to the same legislation and policies as other public records. These include the *Recorded Information Management Policy*, the *NWT Archives Act*, the *Access to Information and Protection of Privacy Act* and the *Government Security Policy*. Refer to *Appendix A, Laws and Policies Related to E-mail* for more detail.

1.5 Background

Like other organizations, the Government of the Northwest Territories is sending more information in electronic format than traditional paper format. This requires the application of good information management practices in the creation, use, and management of e-mail messages, including the identification and retention of e-mail messages.

Good information management practices also facilitate the sharing and distribution of information across divisions and departments of the GNWT regardless of the format of the information.

The following effective information management practices will enable the GNWT to meet legislative, business, and accountability requirements. These practices can save the GNWT considerable expense and time to conduct searches of back-up tapes and e-mail systems in the event of a lawsuit or a request made under the *Access to*

Information and Protection of Privacy Act. In addition, these practices can save the GNWT embarrassment by curbing inappropriately written messages, which may have to be released in such cases.

1.6 Definitions

Administrative Records are records common to all offices and which are distinct from operational records. Administrative records support "housekeeping" functions such as the management of facilities, property, material, finances, personnel and information systems. Administrative records also relate to common management processes including committees, agreements, contracts, information services, legal opinions, and other similar functions.

Administrative Records Classification System (ARCS) is the government-wide standard for the classification, filing, retrieval, retention, and disposition of all types of administrative records. (RDA # 1995-32)

Attachments are those documents appended to and sent with an e-mail message such as word processing documents, spreadsheets, sound files, image files, etc. They form a central part of an e-mail message, and both the message and the attachments form an e-mail record.

Electronic mail (e-mail) messages are communications created, sent, or received on an electronic mail system and include any attachments transmitted with the message as well as the associated transmission and receipt data. E-mail messages include those sent or received internally or externally.

Electronic mail (e-mail) system are computer applications used to create and receive electronic messages, and to transmit electronic messages and any other electronic documents in the form of attachments between individual users and/or groups of users.

Life-cycle means the span or time from the creation or receipt of a record through its useful life to its final disposition.

Listserv is a small computer application that automatically sends out e-mail to names on a mailing list. When e-mail messages are sent to a LISTSERV mailing list, they are automatically broadcast to everyone on the list.

Metadata (i) data describing the context, content, and structure of records and their management through time. (ii) metadata is **not** part of the content of a record, but it is generally the hidden data captured during transactions, such as the date and time that someone received an e-mail message. Metadata helps provide context to records

and answers the questions of who, what, why, when, and where in order to establish integrity and authenticity.

Operational Records are those records which relate to the operations and services provided by a department or agency in carrying out the functions for which it is responsible according to statute, mandate, or policy. Operational records are distinct from administrative records and are unique to each government organization.

Operational Records Classification System (ORCS) is the government-wide standardized system for the classification, filing, retrieval, retention and disposition of operational records. Each department, agency, board, or crown corporation will have one or more ORCS.

Postmaster is the capability in a program, usually a special program designated as an e-mail server, for handling the distribution, forwarding, and receiving of e-mail in a network.

Public Record includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microfilm, sound recording, video tape, machine-readable record, manuscript, inventory, pamphlet, periodical, photographic slide, micrographic, electronic data print-out, and any other documentary material, regardless of its physical form or characteristics, held by or under the control of a government body. [S.N.W.T 1999, c. 21, 5.2(2)]

Recorded Information (records) means information in any form, including electronic records, and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or other mechanism that produces records. [IPC Policy 6003.00.18 – GNWT Recorded Information Management Policy]

Transmission and Receipt Data include such things as originator, recipients, carbon copy (cc), blind carbon copy (bcc), subject, date and time. These data are an integral part of an e-mail message and form part of the e-mail record.

Transitory records are those records that are needed only for a limited time for the completion of a routine action or to prepare a subsequent record. Transitory records do not include records required by government organizations to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of government.

2. *Creation and Use of E-mail*

Use of e-mail, like any form of communication, must consider the rules of etiquette. There are common courtesies and customs that employees are required to follow. Refer to *Appendix B, E-mail Etiquette Guide*.

2.1 Selection and Use of E-mail

E-mail provides an ideal tool to quickly and easily communicate and share information. Employees can use e-mail to:

- Send out administrative and corporate communications through GNWT distribution lists;
- Share project-related information and reports within and between work groups;
- Share committee agendas and minutes;
- Circulate draft documents;
- Replace telephone calls, particularly between personnel working in different regions;
- Set up meetings, appointments and work schedules; and
- In some cases, action informal approval processes.

There are certain instances where employees should select a more appropriate means of communication. For example, employees should NOT use e-mail:

- If a more time-effective or cost-effective communication method is available, for instance, when a telephone conversation would be quicker;
- As a replacement for manager-subordinate face-to-face communication;
- For personnel performance-related communications;
- If confidentiality and privacy are required.

2.1.1 Misuse of E-mail

E-mail should be used in a considerate and responsible manner while respecting the needs and rights of others, and in accordance with the Use of Electronic Mail and the Internet Guidelines. There are many ways to misuse e-mail such as:

- Adding comments that may be uninformed or offensive, and that would not be written in an office memo;
- Making a statement about or to someone that one would not make face-to-face with the person;
- Sending messages and/or attachments that contain abusive, racist, sexist or sexually explicit content or pictures;

- Sending junk mail, unsolicited material, or chain letters. These are intrusive to recipients, may be seen as threatening, and can cause excessive loading of mail facilities. Forwarding spam or chain letters is considered misuse of e-mail.

E-mail misuse can contravene territorial government policy, guidelines or legislation, the Human Rights Act, or the *Criminal Code of Canada*. Depending on the nature and severity of this misuse, it can lead to disciplinary action, criminal charges or lawsuits.

2.2 Legal Issues

Employees' e-mail messages that contain evidence of business decisions, actions, and transactions are a legitimate source of evidence. Rules of disclosure for e-mail messages are the same as for paper records. This means that organizations can be obliged to supply e-mail messages in the event of a legal dispute. This can include messages regardless of the medium on which they are stored (hard copy, hard drives or networks).

Employees must use e-mail in compliance with Territorial laws and regulations. Activities such as sending out messages that promote hatred against identifiable groups or an individual, distributing obscene material, or violating another person's copyright, are unlawful. Such activities could result in sanctions of different kinds in a court of law.

2.3 Access

E-mail messages that employees create, send or receive in the conduct of GNWT business must be accessible, so that they can be used as required for business-related purposes, and to meet legislative and GNWT accountability requirements. For this reason there must be regular maintenance, organization, and filing of employees' e-mail messages and the regular deletion of employees' e-mail transitory messages and other types of information not related to the GNWT's business.

The public can gain access to employees' e-mail messages under the *Access to Information and Protection of Privacy Act*. This includes all e-mail messages that employees have created, sent or received using the GNWT e-mail system.

2.3.1 Access to Employees' E-mail by Administrators

The GNWT E-mail Administrator or Technology Service Centre Administrator may be asked to access employee e-mail accounts. This will be done only in limited circumstances, as follows:

- With the employee's consent to fix a problem;
- With the supervisor's consent to access a specific business related e-mail, in a situation when the employee is away from the office or unavailable and where the e-mail is otherwise inaccessible and is required;
- In response to a legal investigation;
- During an investigation of suspected misuse of e-mail or other authorized investigation; or
- Under an Access to Information and Protection of Privacy request.

By applying any of the options as identified in *Appendix D, Filing E-mail Messages*, the need to access employees' e-mail accounts by a GNWT E-mail Administrator will be limited.

2.4 Privacy

Employees must seriously consider privacy and confidentiality when choosing e-mail as a means of communication. The GNWT e-mail system does not currently provide security features to protect e-mail messages during transmission. Refer to *section 2.5, Security*.

Choosing e-mail to send personal information about an individual or employee, or to send information that is security classified, greatly increases the chance of unauthorized disclosure. Employees' messages could be intercepted in transit or be read by someone else. Employees must keep in mind that e-mail messages can easily be forwarded to others or could even be delivered to the wrong address.

Remember that all e-mail messages created or received by employees using the GNWT e-mail system can be accessed under the *Access to Information and Protection of Privacy Act.* As well, other individuals in the organization have a right of access to information, including e-mail messages, that pertain to the business of the organization. Employees should have **NO** expectation of privacy when it comes to e-mail messages they create or receive.

2.5 Security

As outlined in the *GNWT Security Policy*, sensitive government information must be protected and access to it must be controlled.

The GNWT e-mail system does not currently have enabled security features such as the ability to digitally sign and/or encrypt e-mail messages and attachments. Without protection, information sent electronically can be easily compromised. A key concern is the chance that an e-mail message may never reach its intended recipient and the sender may be unaware of that fact. Employees must always use e-mail with the assumption that messages may be read by someone other than the intended recipient.

Until suitable security features are made available for e-mail messages, employees should not:

- Transmit any e-mail messages they would not want someone other than the intended recipient to see;
- Transmit security classified or designated information by e-mail.

Employees are responsible for the e-mail messages they create. To help ensure the integrity and authenticity of employees' e-mail messages, employees must ensure that their computer is not left unsecured and that password(s) are not shared with others.

3. Responsibilities

Responsibility for the appropriate creation, use and management of e-mail should be taken at all levels of the organization. These responsibilities are:

3.1 Individual employees

All staff are responsible for distinguishing between official and transitory records. The latter should be safely deleted as per the Records Retention and Disposal Authority for Transitory Records once their usefulness has passed. Refer to *section 5.2, Retention and Disposition – Transitory E-mail Messages.*

Staff are responsible for moving e-mail messages relating to the business of the GNWT into the department's administrative or operational records classification system (ARCS / ORCS). The department's Records Coordinator can provide advice on how to do this. If users have any doubts about the value of an e-mail message as an official record, they should contact the department's Records Coordinator for advice. **It is better to keep such a message than delete it and lose potentially**

valuable information, and/or face sanctions for the unauthorized destruction of a public record.

When deleting e-mail messages, remember to delete only those messages that are transitory records, not information that is related to the business of the GNWT. Employees must perform regular clean-ups of e-mail by sending e-mail messages to the records classification system and deleting the others. Refer to section *4, Management of E-mail Messages*. Regular clean-ups will allow employees to find and share information faster.

3.2 Managers/Supervisors

GNWT managers are required to ensure that staff are aware of their responsibilities regarding the management of e-mail. Managers and supervisors are required to ensure that their respective employees follow the policies, guidelines, and procedures for the capture and management of e-mail.

3.3 Departmental Records Coordinators

Departmental Records Coordinators are responsible for the overall management and control of the department's records management program. They also provide advice, assistance, and training on department specific records management issues.

3.4 Public Works and Services, Records Management Section

Public Works and Services (PWS), Records Management Section is responsible for developing policies, standards, and guidelines regarding the management of recorded information across government. They also provide advice, assistance, and training on government-wide recorded information management issues.

4. Management of E-mail Messages

It is important to remember that all of the information that employees collect or create in the conduct of business is the property of the Government of the Northwest Territories. As with other types of information, employees must manage e-mail messages with consideration of the legislative requirements, as well as the department's business and accountability requirements.

Employees must retain, organize, and manage e-mail messages that are identified as public records so that employees can easily access and retrieve them. In the GNWT, ARCS and ORCS is used to manage public records.

E-mail messages that are transitory records should be deleted once this information is no longer of use to employees. Refer to *section 5.2, Retention and Disposition – Transitory E-mail Messages.*

The distinction between an official record and a transitory record may be difficult to determine. If there is any doubt, employees must consider the e-mail message as an official record, and retain it in an appropriate manner.

4.1 E-mail Messages

4.1.1 Determining which e-mail messages are records

An e-mail message is considered to be a record if it was created, sent or received in order to control, support, or document the delivery of GNWT programs, to carry out operations, to make decisions, or to account for activities.

The following e-mail messages are examples of official records:

- Messages that reflect the position or business of the GNWT;
- Messages that initiate, authorize or complete a business transaction;
- Messages received from external sources that form part of a public record;
- Original messages of policies or directives;
- Original postmaster messages; and, where the information does not exist elsewhere:
- Messages related to work schedules and assignments;
- Agenda and minutes of meetings;
- Briefing notes;
- Final reports and recommendations.

4.1.2 Responsibility for keeping e-mail messages

The onus is on the **originator** of the e-mail message to ensure that the official GNWT e-mail message is kept and filed. If employees are the **recipient** of an e-mail message that is sent from an external source, or, where the information does not exist elsewhere in the department and forms part of the public record, then the e-mail message must be kept and sent to the department's records classification system.

In the case where an employee originates an e-mail message that requires a response from one or more recipients, then the employee who sent the original e-mail message must ensure that the original message and all responses are kept.

4.1.3 Filing e-mail messages

It is recognized that there is often a need for workers to hold on to e-mail messages that are public records until they have served their primary purpose. However, once the primary purpose has been served, the e-mail message must be sent to the department's records classification system.

Employees must file e-mail messages in the department's records classification system under the following circumstances:

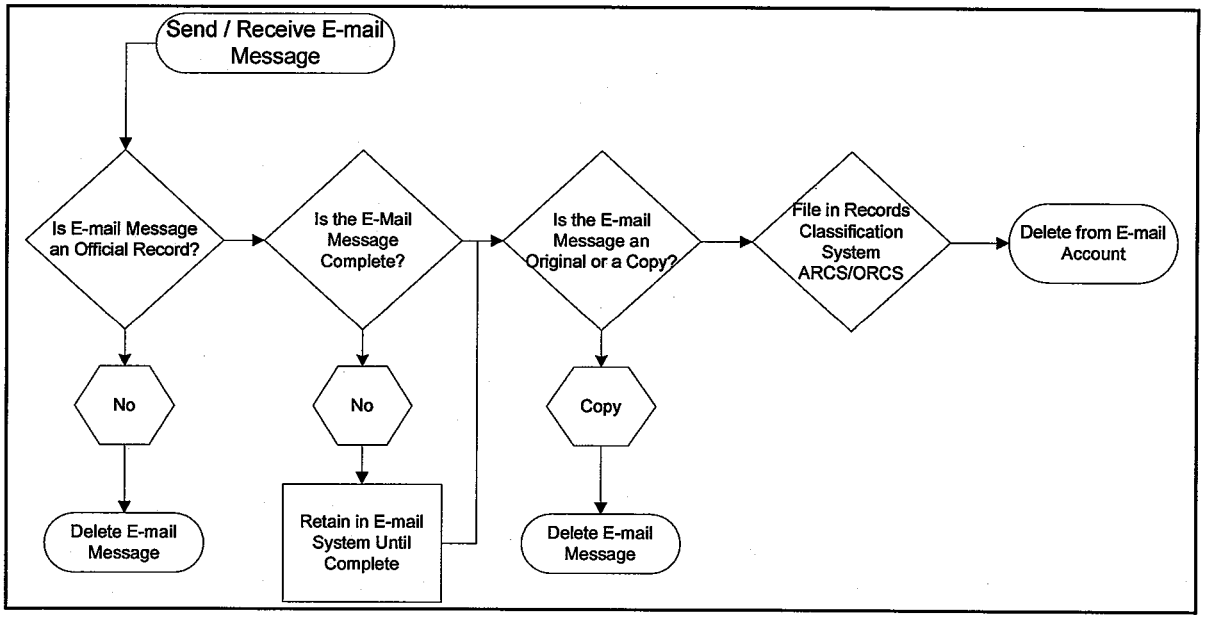
- When all actions associated with the content of the e-mail message have been completed;
- When there is a need to share the e-mail and/or it's attachments with other employees; and
- When the recipient has the final and complete version of the e-mail (when the e-mail chain is complete).

4.1.4 Managing copies of e-mail messages

E-mail messages received internally through the Postmaster or other GNWT distribution lists, are considered transitory records. Employees may delete these messages once this information is no longer of use to employees. The onus is on the originator to ensure that the original messages are retained as public records. This would also apply to copies of e-mail messages sent internally between work groups/units, solely for reference or information.
Employees may delete e-mail messages that:

- Contain information from outside sources;
- Were distributed for reference purposes; and
- Are not required to document GNWT business activities.

Figure 1: *E-mail Messages*



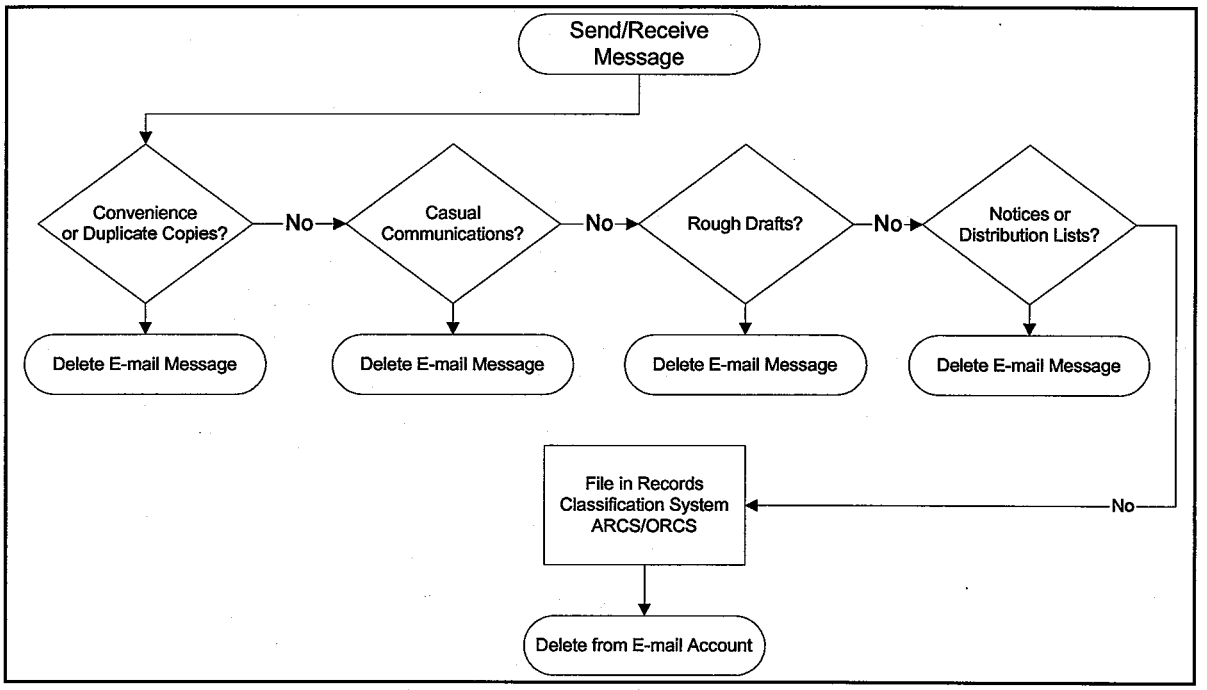
4.2 Managing Transitory E-mail Messages

Transitory e-mail messages are records required only for a limited time to complete a routine action or to prepare a subsequent record. Transitory e-mail messages 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 GNWT. They are described and scheduled in the Transitory Records Schedule (RDA # 1997-02). Transitory e-mail messages may include:

- Messages that are copies of information used only for convenience of reference and not as the official record;
- Messages used for casual communication such as requests to attend meetings, working groups, etc.;
- Informal messages or rough drafts that are not required to document the development of a public record;
- Messages that are duplicate copies of information;
- Miscellaneous notices of employee meetings, holidays, etc.;
- Messages received as part of a distribution list or received from listservs.

Employees must not delete transitory records where the GNWT has received a formal request, made under the *Access to Information and Protection of Privacy Act*, relating to these records.

Figure 2: Transitory E-mail Messages



5. *Retention and Disposition*

By law, employees must not destroy public records without the consent of the Public Records Committee (PRC) as per the *NWT Archives Act*. This is to permit the identification and preservation of archival and historical records. The authority to dispose of records is granted by the PRC through the approval of Retention Disposition Authorities also known as records retention and disposition schedules.

5.1 E-mail Messages

As with other types of public records, e-mail messages have various retention periods. Retention periods vary according to the function and content of the record, and can range from short term (e.g., six months to one year) up to long term (e.g., when operational requirements cease).

A Records Disposition Authority identifies categories of records that are eligible for disposition once they have been kept for a specified period of time. An approved Records Disposition Authority indicates that both the department and the Territorial Archivist have approved the final disposition of the records.

A single Records Disposition Authority, the GNWT Administrative Records Classification System (ARCS), applies to all administrative records held by GNWT agencies. In addition to ARCS, each department or agency will have one or more records disposition authorities for their unique operational records. Records Disposition Authorities for operational records are known as Operational Records Classification Systems (ORCS).

Records Disposition Authorities, ARCS and ORCS, apply to both paper-based records and e-mail messages maintained in electronic format. The disposition of e-mail messages, like their paper counterparts should be managed under the direction of trained records management personnel.

5.2 Transitory E-mail Messages

Employees may delete e-mail messages they have determined to be transitory records once they are no longer of use to employees. **Remember, employees must not delete transitory records where the GNWT has received a formal request, made under the *Access to Information and Protection of Privacy Act*, relating to these records.** Refer to *section 4.2 Managing Transitory E-mail Messages.*

6. *Enquiries*

Enquiries about these guidelines or the application of these guidelines should be directed to Departmental Records Coordinators and/or the Records Management Section, PWS. Any technical questions related to email applications should be directed to the Technology Service Centre.

Appendix A - Laws and Policies Related to E-mail

Whatever the form, records under the control of government departments must be managed in accordance with existing laws and policies related to information. Some of the key laws and policies, relevant to the management of government information are listed below:

The ***NWT Archives Act*** prohibits the destruction of government and ministerial records, or their removal from the control of the government, without the consent of the Public Records Committee. Departments are also required to transfer information holdings determined to be of historical or archival importance to the NWT Archives in accordance with schedules or agreements.
http://www.justice.gov.nt.ca/PDF/ACTS/Archives.pdf

The ***Access to Information and Protection of Privacy Act (ATIPP)*** provides the public with a right of access to public records. ATIPP makes government departments accountable for the information they control and for providing access to it (except in limited circumstances as defined in the *Act*).
http://www.justice.gov.nt.ca/PDF/ACTS/Access_to_Information.pdf

The ***GNWT Electronic Information Security Policy*** identifies requirements to ensure that all classified or designated information of the territorial government is safeguarded in an appropriate manner.

The ***GNWT Policy on the Management of Electronic Information*** provides guidance and helps departments manage their recorded information. It assigns responsibility for managing recorded information to the department that created or acquired the recorded information. It also establishes a framework to promote cooperation on government-wide issues and public policy issues related to recorded information management.
http://www.pws.gov.nt.ca/pdf/recordsManagement/RM_policy_NWT_final.pdf

The ***GNWT Use of Electronic Mail and the Internet*** defines and explains proper use of the Internet and electronic mail (e-mail) by employees of the GNWT and provides guidance to employees regarding appropriate use of the government Internet and e-mail systems.
http://www.gov.nt.ca/FMBS/documents/dox/internet-email.pdf

Appendix B - E-mail Etiquette Guide

1. Always include a clear and unique subject heading. This allows for easy filing, cataloguing, cross-referencing and retrieval. Ensure that the subject line reflects the body of the e-mail. You may wish to use a keyword or subject at the start of the subject line to facilitate sorting.

2. Keep messages reasonably short. Too much information in one message is a burden on recipients.

3. Consider the readability of the message. Use short lines and paragraphs, or present information in point form. Use correct grammar and check the spelling of messages before sending.

4. Do not write with uppercase letters only and limit the use of exclamation marks. Uppercase letters are difficult to read, and some recipients may consider it shouting. If visibility is an issue, increase the font size.

5. Keep it clear--specialized terminology, acronyms and other jargon may detract from the readability of a message. Remember that you may be sending messages to readers with varying backgrounds or levels of expertise.

6. Send "carbon copies" (c.c.) to others who may be affected by the e-mail message or who may have information or suggestions to add.

7. Acknowledge text that is not your own and do not make changes. Your alterations to another person's text could confuse the original meaning.

8. Allow enough time for the respondent to research and formulate a response. If your message needs an answer within 24-hours, you can inform the recipient by other means, such as a telephone call. This will reduce the need to monitor inboxes.

9. Respond to e-mail messages as quickly as possible. If necessary, send an acknowledgment to let the sender know if your answer will require a few days. Trivial responses or unnecessary replies should be avoided.

10. Do not forward e-mail inappropriately. Do not forward another person's message to others without that person's permission.

    Do not forward e-mail unnecessarily. Pay attention to the recipient list before forwarding received mail, as the recipient may have a copy already. As a rule use

the "reply to sender" option; use the "reply to all" option only when return message apply to all recipients.

11. Respect copyright. If you are sending information quoting the writing of another person or organization, it may have copyright protection. Copyright laws apply to e-mail and may restrict the copying or use of the information (check with your department copyright expert.)

12. Mark e-mail as *urgent* (high priority) only when *urgent*. Do not cry wolf!

13. Use language that is business-like and professional. Remember that e-mail messages are public records. Do not say anything in an e-mail message that can't be made public, put on file, or forwarded to others. Use humour with care as it can easily be misinterpreted.

14. Using abusive or offensive language in an e-mail message is inappropriate. Do not write anything you would not say face-to-face.

15. Avoid public "flames". Messages sent in the heat of the moment usually worsen the situation and are regretted. Delay responding to any message that angers or upsets you, and consider talking it over with colleagues or your supervisor before your reply.

16. Be aware that e-mail works through shared technology. If confidentiality and privacy are required, use a more appropriate communication method.

17. If the document is intended to be read only through e-mail, avoid the use of file attachments. Attachments add unnecessary bulk and make it more difficult and time consuming to read. Use text in the body of the message when possible.

18. Limit the number and size of attachments. If you are having problems sending a large file, contact Systems and Communications, PWS, for information on how to transfer oversized files.

19. Don't send junk mail, chain letters or any other unsolicited material such as repetitive mass mailings or advertising. This unnecessary distribution can cause excessive loading of mail facilities, and is an inappropriate use of your time. Chain letters can also sound threatening to some.

Appendix C - E-mail FAQS
(Frequently Asked Questions)

1. Do I have to treat my e-mail messages as public records?

YES
All e-mail messages sent or received on the government e-mail system are "public records" as defined by the Archives Act. They are also known as "government records." Some are "official" records and some are "transitory."

"Official records" are those required by the GNWT to control, support, or document the delivery of programs, to carry out operations, to make decisions. (see section 4.2) Also known as substantive records.

"Transitory records" are messages that do not serve these purposes and have no enduring value; this includes information provided for reference purposes or announcements not related to GNWT business (see section 4.2)

If you can not determine the status, you should treat the message as an official record. If part of the message is official and the rest is not, the whole message must be managed as an official record.

2. Who should be filing e-mail messages?

IT DEPENDS
If you sent the original message, you are responsible for making sure that the message is filed in your department's records classification system (ARCS/ORCS).

If you receive a message, and you are the only recipient in your division, then it is your responsibility to make sure that the e-mail message is filed. If you are one of several recipients in your division, speak to your Departmental Records Coordinator to find out how your department is filing e-mail messages. There are three main options that departments may use:

- The first recipient in the division (e.g. the first person in the To: line) is responsible for making sure that the e-mail message is filed.
- All messages are sent to someone in the division who has been designated responsible for filing the division's e-mail messages. This can be done by forwarding the message to that person, or by saving the message into a shared e-mail folder.
- All employees file their e-mail messages. The rationale behind this option is that it is better to have duplicate copies filed than to have an incomplete record.

3. **Must I keep all the e-mail messages that I create or collect?**

   IT DEPENDS
   Should an employee's e-mail message fall under the definition of an official record, it must keep it to meet legislative requirements, and GNWT business and accountability requirements. Should the e-mail message fall under the definition of a transitory record or another type of information not related to the GNWT's business, it can be deleted once it is no longer of use. Refer to *section 4, Management of E-mail Messages, section 4.1, E-mail Messages* and *section 4.2, E-mail Transitory Messages.*

4. **Is it acceptable for me to use the GNWT e-mail system for personal communications?**

   NO
   According to the *GNWT Use of Electronic Mail and the Internet Guidelines*, personal use of the GNWT electronic networks, which include the e-mail system, is not permitted.

5. **Is my e-mail private?**

   NO
   E-mail messages created or received by employees using the GNWT e-mail system can be accessed under the *Access to Information and Protection of Privacy Act* or in the event of legal action. As well, other individuals in the organization have a right of access to information, including e-mail messages, that pertain to the business of the organization. Employees should have **NO** expectation of privacy when it comes to e-mail messages they create or receive.

6. **Must I provide non-business related e-mail messages upon a request under the *Access to Information and Protection of Privacy Act*?**

   YES
   It is important to remember that employees have to provide all e-mails that are pertinent to the request (sent and received). If some of the e-mails contain information on the request as well as non-business related information, they must be submitted to the GNWT *ATIPP* Coordinator for review. If applicable, the exemptions under the Act will be applied to the information; if none apply it will be released to the applicant.

7. When I provide an e-mail message in response to a request under the *Access to Information and Protection of Privacy Act*, can I remove any personal comments?

NO
Upon receiving a request under the *Access to Information and Protection of Privacy Act*, all e-mail messages must be kept in their original format, including any written personal comments. If applicable, exemptions will be applied on the personal comments; if none apply it will be released to the applicant.

8. I deleted an e-mail message. It no longer exists, right?

NO
Even after employees have deleted them, e-mail messages may still be stored on GNWT file servers or back-up tapes. Back-ups are performed on the e-mail system on a regular basis. Also, other recipients or senders may keep electronic or paper copies of the e-mail messages, and/or may have forwarded them to others.

9. What should I do if I receive an inappropriate e-mail message?

Should you receive e-mail you feel is inappropriate such as messages containing abusive, racist, sexist or sexually explicit material, you should inform your supervisor or manager. He or she may contact the GNWT Human Resources Office and/or the Audit Bureau. Depending on the nature and severity of this material, it may be a matter that requires investigation by one or both of these offices.

If you receive e-mail spam (unsolicited advertising, junk mail) or a chain letter, do not forward it to others or reply to it. You are responsible for it and should delete it immediately.

10. What should I do with my e-mail messages when I am leaving the GNWT or transferring within the GNWT?

Prior to leaving the GNWT or transferring to another department or division within the GNWT, you must perform a clean up of all your e-mail messages in the current e-mail program or, if applicable, in network directories, on your local hard drive or on diskettes, etc. You must retain and send to the department's records classification system all those messages determined to be public records. Refer to *section 4.1, E-mail Messages*.

Employees can accomplish this by using one or more of the following options:

- Filing e-mail messages in electronic format within a shared directory in the appropriate directory files (if your area is using a shared directory),
- Transferring e-mail messages to another responsible person,
- Printing and filing e-mail messages in the applicable records office or in any other applicable filing area for hard copy records.

You may delete all those messages you determine to be transitory records and other types of information not related to the GNWT's business. Refer to *section 5.2, Retention and Disposition – Transitory E-mail Messages.*

Before conducting the clean up of your e-mail messages, you must consult with your GNWT Records Coordinator to determine and agree upon the filing method for your e-mail messages.

11. What about encrypted e-mail messages?

The GNWT e-mail system does not currently provide the ability to encrypt e-mail messages. If you are using encryption, you are responsible to ensure that decryption keys are available to those who will need to access to your GNWT e-mail messages. It is recommended that you file and store these records in a decrypted format. E-mail messages should be decrypted before being transferred to NWT Archives for final disposition.

Appendix D - Filing E-Mail Messages

Key concerns when filing e-mail messages, including attachments, is the ability to identify, retrieve and share this information, as required. Messages identified as official Public Records should be filed; those considered transitory records should be deleted. Refer to *section 4, Management of E-mail Messages*.

It is unnecessary to keep several duplicate copies of the same e-mail message within the same division. However, if employees have added information to the e-mail message, it is considered to be a unique original and the employee must keep it.

It is unnecessary to keep e-mail messages in more than one format. If employees have printed and filed e-mail messages in hard copy they can delete the electronic copy. If employees have copied and filed e-mail messages in a shared directory, the copy in the current e-mail program can be deleted. Keeping both electronic and hard copy of the same record brings the reliability and authenticity of the record into question.

Recommendations

Employees file e-mail messages so that they can reproduce and view them in their original electronic format, (whether this is the actual current e-mail program message along with its transmission and receipt data, or an attachment such as a Microsoft Word or Excel document).

Filing and storage for electronic records must be based on the area's file classification structure – ARCS and ORCS. This will enable employees to maintain a link between messages and attachments, and any other related records.

Electronic Document Management System

An Electronic Document Management System (EDMS) captures and stores electronic documents and e-mail messages in a central repository. It allows employees to assign various attributes to the message such as a document title, subject and description, and access rights by others. As well, the system will automatically assign such information as employees' names, department, division, the document application type, etc., to each message. Employees can then research and retrieve documents based on these attributes, as well as using full-text searches. They can retrieve both their own documents and others in the categories to which they have access.

An EDMS, such as iRIMS (records management software manages the records life-cycle for both electronic and hardcopy records), provides greater control for the management, identification and retention of a department's electronic documents and e-mail messages,

and allows for the life-cycle management of this information in electronic format. It also facilitates the sharing of this information with broader audiences.

Options for Filing E-mail:

Microsoft Outlook

Microsoft (MS) Outlook provides the ability to create folders and sub-folders, which allow employees to organize and manage their e-mail messages in the original format.

Employees can create these folders directly in their Outlook mailbox or use public and personal storage folders. Public and personal storage folders allow employees to store e-mail messages on shared network servers or on employee's local hard drive.

Recommendations

Employees must use the LAN server for e-mail storage. Information stored on the local drive is not automatically backed up; employees are responsible to ensure adequate back up of their local drives.

Employees may wish to organize their e-mail messages in public or personal storage folders modeled on the file classification system structure (ARCS/ORCS) already in use for other records. This will maintain a link between e-mail messages and any other related records. Public storage folders permit employees to share documents with defined work groups or committees, or with as broad an audience as all GNWT employees.

Shared Directories and Files

Employees can manage e-mail messages in electronic workspaces through the use of shared directories and files on the network. Employees should establish these electronic workspaces based on their division or program area's file classification structure (ARCS/ORCS). This will maintain a link between messages and attachments, and any other related records. Restrictions can be put in place to limit access so only those authorized to work on the file can see the information. (If employees need help establishing a file classification structure (ARCS/ORCS), they should contact their departmental Records Coordinator or the PWS Records Management Division.)

There are three format options for saving messages from MS Outlook into shared directories: .txt (Notepad), .rtf (Microsoft Word), or .msg (MS Outlook).

Recommendations

Save e-mail in its MS Outlook format (.msg). This will allow employees to reproduce the e-mail in its original format and will ensure the capture of its metadata and any attachments.

Saving in Notepad or Microsoft Word format will capture the transmission and receipt data, but employees will have to save attachments as separate documents.

Converting to any format outside Outlook is not recommended as the integrity of the original e-mail message may be compromised during conversion.

Records Offices and Hard Copy Files

If no other option is available, to ensure the retention and filing of e-mail messages in an appropriate GNWT classification system, employees may print e-mail messages for filing within the applicable records classification system (ARCS/ORCS) for hard copy records. The loss of transmission and receipt data (metadata) is a concern for the evidential value of printed copies of e-mail messages. If not sure, employees should consult their information systems personnel to ensure that all metadata are printed with the messages.

Appendix E - Removal of Employees' E-mail Accounts

A GNWT E-mail Administrator will remove the employee's e-mail account from the network after a specified period from the date the employee leaves the GNWT. This is accomplished by:

- Verifying with the employees former Manager or the Departmental Records Coordinator that all public records have been removed and obtaining his/her documented approval to permanently remove employees e-mail account.

- If necessary, retaining employees' e-mail accounts either on the network or on another media such as on CD, until the e-mail messages are processed for retention.