Information Management

Managing Electronic Mail in the Government of Alberta

February 2005

GOVERNMENT OF ALBERTA

Produced by

Information Management Branch
Government and Program Support Services Division
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web sites:
http://www.im.gov.ab.ca
http://www.gov.ab.ca/foip
http://www.pipa.gov.ab.ca

 ISBN 0-7785-3692-0

Contents

1. INTRODUCTION

Electronic mail (e-mail) is an integral part of doing business today and has replaced a large number of telephone calls, memos and letters.

Although e-mail has helped improve business communications, it is a significant contributor to the perception of "information overload." Many people are unsure of how to manage their e-mail effectively: they don't know what to keep, what to delete, and how to organize the messages they do keep.

It makes good business sense to manage e-mail records. For government, it is also a legislated requirement.

Purpose

The purpose of this guide is to

- bring together existing policies and legislation that govern the management of e-mail in the Government of Alberta;
- describe guidelines and practices that should be established at the ministry level; and
- provide some tips to help individual employees manage e-mail more effectively.

The advice provided will help ministries develop effective practices that comply with relevant legislation related to government records, including the following:

- *Records Management Regulation* governs how records must be managed and the process for approving how long they must be retained. This Regulation also governs the disposition of records – either through destruction, or transfer to the Provincial Archives of Alberta.
- *Historical Resources Act* establishes the Provincial Archives and governs the permanent preservation of government records of archival value to ensure they are available to Albertans in the future.
- *Freedom of Information and Protection of Privacy Act* (FOIP) governs the collection, use and disclosure of personal information, how personal information must be handled and protected, and the right of the public to access records in the custody or under the control of ministries.
- *Health Information Act* governs the collection, use and disclosure of health information, how health information must be handled and protected, and the right of the public to access health records in the custody or under control of health care providers defined under the Act, including the Ministry of Health and Wellness. The Act does not apply to health records retained by other ministries.
- *Electronic Transactions Act* gives electronic signatures and records the same legal status as their paper-based counterparts.

- *Alberta Evidence Act* provides rules on the admissibility of paper records in court proceedings. The *Act* also includes electronic records.
- *Government Emergency Planning Regulation* requires ministries to create plans for business resumption, including the identification and handling of records needed for business resumption after emergencies and the protection of assets, financial records and other records maintained by the ministry.

All of this legislation means that ministries must have in place recordkeeping practices and procedures. This document places e-mail within the context of these requirements.

Scope

These policies and guidelines apply to all authorized users of Government of Alberta e-mail systems. They apply whether the user is using government equipment, their own equipment, or equipment belonging to a third party.

Electronic mail or "e-mail" is electronically transmitted information created on, or received by, a computer system. An e-mail message consists of at least three components – the "envelope" or mail header data, the message content, additional information (metadata) in the message "properties" and frequently attachments as well.

Implementation

These policies and guidelines form part of the government's broader Information Management Framework being co-developed by the Office of the Corporate Chief Information Officer and Government Services. Implementation details will depend on each ministry's individual business requirements, organizational culture and technology architecture.

Overview

This guide contains three main sections:

- The Government of Alberta Policies on E-Mail describes existing government policy and legislation that affects the management of e-mail.
- Establishing E-mail Guidelines and Practices in Ministries provides advice on best practices related to managing e-mail within individual ministries. Ministries are responsible for developing appropriate recordkeeping systems and user guidelines that include the handling of e-mail records.
- Managing E-Mail at the Desktop identifies practices that can help individual employees manage e-mail on a regular basis, whether at their desk or using mobile computing technology.

The policies and guidelines are accompanied by some useful tools in the appendices to this guide including:

- Identifying and Deleting Transitory Records: Employees can use this diagram to help them decide which records they must retain and integrate into their ministry's records management systems and which records they may delete.

- Ten Ways to Make E-Mail Effective: Contains some practical advice to help make e-mail effective and to reduce information overload.

- Sample Ministry Guidelines and Practices: Shows one example of best practices at the ministry level for documenting practices and responsibilities to help employees manage e-mail.

- Glossary: Defines some of the terms used in the policies and guidelines related to managing e-mail messages as records.

- Resources: A list of useful resources related to the management of e-mail.

Note: Several documents listed in this document are available on the Shared Repository (SHARP) (http://www.sharp.gov.ab.ca). This site is accessible to Government of Alberta employees (firstname.lastname@gov.ab.ca) and also to extended stakeholders (i.e. agencies, boards and commissions), consultants contracting with the Government of Alberta and employees of other governments who are registered users of the SHARP web site.

2. GOVERNMENT OF ALBERTA POLICIES ON E-MAIL

Several policies relate to the use and management of e-mail in the Government of Alberta. These policies concern

- the authorized use of the Government of Alberta e-mail systems;
- the acceptable use of e-mail;
- the transmission of personal information via e-mail; and
- managing e-mail as records.

Authorized use of Government of Alberta e-mail systems

Access to Government of Alberta e-mail systems will be based on business needs and will normally be provided to all employees of the Government of Alberta.

The Government of Alberta Information Technology Security Policy allows access to government e-mail systems by staff of other organizations if there is a clear business need for the services and the individuals are contracted by or acting as an agent for a ministry.

Acceptable use of e-mail

The Government of Alberta Internet and E-Mail Use Policy describes the conditions of use by Alberta Government employees of both the Internet and e-mail. Key components of this policy are:

- Authorized users of government e-mail systems are encouraged to use e-mail systems and tools to fulfil their employment duties and to support their ministry's business goals.
- Personal use of e-mail systems is permitted, provided the use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain.
- Users must not bring disrepute to the Government of Alberta.
- Use of the network and e-mail must not conflict with responsibilities outlined in the Official Oath of Office and the Code of Conduct and Ethics for the Public Service of Alberta.
- Users must not violate applicable laws and are expected to use discretion and good judgement when using e-mail systems.
- All users, including remote access users connecting to government systems through the Internet, must take reasonable precautions to safeguard government systems and not to cause damage to government systems.
- Ministries may initiate investigations of e-mail use as warranted.

Transmission of personal information via e-mail

The Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile was adopted by Deputy Ministers in September 2001 and later updated in July 2002 to include implementation guidelines for ministries.

The policy states that any documentation or records containing personal information must not be externally transmitted by electronic mail or facsimile unless

- personal identifiers have been removed;
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other means are employed by both the sender and the recipient to ensure confidentiality is maintained.

The policy also requires that

- automatic address substitution should not be used (e.g. some Internet Service Providers configure e-mail systems to resend mail to another address that may be similar such as joe@xyz.com instead of jo@xyz.com); and
- a statement about inadvertent transmission and receipt should be attached to all e-mail messages sent outside of the Government of Alberta that contain sensitive, personal, confidential or privileged information (e.g. This communication is intended for the use of the recipient to whom it is addressed, and may contain confidential, personal and/or privileged information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. A communication received in error, or subsequent reply, should be deleted or destroyed).

Further details about this policy and its implementation are available from the Office of the Corporate Chief Information Officer.

Managing e-mail as records

In addition to these policies, various statutes and regulations affect the management of e-mail records.

E-mail messages created or compiled on, or sent or received on Government of Alberta e-mail systems are records of the government. These records

- are the property of the Government of Alberta;
- must be managed according to the provisions of the Records Management Regulation and any records management policies, standards and procedures issued by the Alberta Records Management Committee (ARMC) and Alberta Government Services (the ministry responsible for the government's records management program); and

are subject to both the access provisions and the protection of privacy provisions of the *Freedom of Information and Protection of Privacy Act*.

Ministries are responsible for collecting, creating and capturing records that adequately and properly document their organization's

- functions;
- policies;
- decisions;
- procedures;
- resource expenditures;
- operations; and
- delivery of services.

Ministries are also responsible for storing, organizing and retaining these records in such a way that they are available for

- planning and decision-making;
- program and service delivery;
- meeting their obligations to the Legislature to account for their activities, including audits where applicable;
- meeting requests for access to government records by the public, business and other external groups; and
- recovery and business resumption in cases of emergencies or disasters.

Like other records, e-mail records must be managed to meet these requirements.

3.
ESTABLISHING E-MAIL GUIDELINES AND PRACTICES IN MINISTRIES

Records in e-mail systems can be managed successfully by application of a combination of policies, management procedures, systems design and user training.

> E-mail is no longer a messaging system. It is a record-generating and communicating system vital to the business process. The question is whether it is being managed with the same thought and attention that go to other record-generating media.
> (Ken Withers, "Managing Electronic Mail: The Legal Case," 2001)

Ministries should establish clear guidelines and practices for managing e-mail relating to

- integrating the management of e-mail with other records and information management practices;
- protecting the security of the e-mail system and messages;
- ensuring the reliability and authenticity of e-mail records;
- compliance with freedom of information and protection of privacy requirements;
- the ministry's practices for monitoring e-mail; and
- roles and responsibilities for managing e-mail.

The development of such guidelines will require a team approach with the involvement of various groups including IT, FOIP, records management, human resources and business units. See the Sample Ministry Guidelines and Practices (Appendix 3) for an example of how such guidelines and practices can be brought together in a simple form. Ministries should ensure the guidelines and practices are communicated to staff and that training is provided, as needed.

Integrating the management of e-mail with other records and information management practices

The management of e-mail records should be integrated with other records and information management practices for records in the custody or under the control of each ministry.

The best way to do this at the present time is to implement Electronic Information Management (EIM) applications that are designed to manage electronic records through their lifecycle. These types of systems can integrate records management and desktop applications, so that the ongoing capture, organization, retrieval and disposition of electronic records become a routine part of electronic work processes. A corporate Electronic Information Management (EIM) initiative is under way to define GoA requirements and to establish common support tools and practices.

Depending upon the specific applications, EIM technology can address document naming conventions, version control, authentication, workflow, records classification, security,

privacy, and records disposition according to approved records retention and disposition schedules. Many EIM applications can also handle the management of paper records with file folder and box level information.

The Government of Alberta's Information Management Framework (IMF) supports this approach. As part of the IMF initiative, the Office of the Corporate Chief Information Officer and the Information Management Branch (Alberta Government Services) are undertaking work that will help ministries implement these systems.

Until EIM integrated systems are in place, ministries and employees must use existing technology to manage e-mail records and other electronic records. There are a couple of approaches to do this, and areas will have to examine the advantages and disadvantages of each approach for different groups of records. Most business units will use a combination of:

1. **Printing and filing** e-mail messages in the existing records management system. Most business units still retain the official records of their programs in paper or microfilm form.

2. Organizing **shared electronic directories** in which to file e-mail messages, word processing documents, spreadsheets and other types of electronic records. Many areas find this approach useful for locating documents quickly, sharing information, and work in progress.

The advantages and disadvantages of each follow:

- **Printing and filing e-mail messages in the existing records management system.**

  The advantages of this option are:

  - It is easy to implement, especially where well-designed and well-understood filing systems already exist.
  - It integrates related records and information from multiple sources in one place.
  - E-mail options can be set to automatically print distribution, receipt and other required information.
  - Standards and procedures are already in place both for organizing and for properly disposing of hard copy records.
  - In existing systems for paper records, various drafts, work in progress, background materials and reference copies of documents are usually housed in individual workstations, clearly separated from business unit filing system.

  The disadvantages of this option are:

  - The ability to search for, retrieve, or re-transmit documents electronically is lost when messages are deleted from the e-mail system after printing.
  - The possible perception by program and IT staff that this method does not use technology to advantage.

- **Managing e-mail electronically**. This requires program staff, records management staff and network administrators to work together to plan and design electronic directory structures for the business unit. Often the best approach is to implement a structure that is substantially similar to the existing filing system.

  The advantages of organizing and storing e-mail in shared network directories are:

  - It's generally quick and convenient for users to move e-mail messages to electronic directories, especially with shortcuts to the folders most often used.
  - Users have convenient and consistent access to all the related records in the directories they are authorized to access.
  - E-mail records are more easily searched and can be re-transmitted and printed as needed.

  The disadvantages of managing e-mail electronically are:

  - Unless security conditions are stringent, users could have much easier access to records and information that should not be available to them.
  - Directories that contain e-mail messages and final versions of other electronic records may also contain drafts and background materials.
  - Significant effort is required to manage the retention and disposition of electronic records from shared directories according to approved records schedules and auditable procedures.
  - Unless the business process is fully automated, and all records are in electronic form, it will be necessary to coordinate filing systems for records in paper and other media with those in electronic format; and
  - Migration strategies are required to ensure future readability and security of stored e-mail records.
  - Any electronic folders with records that have archival value cannot be preserved in the Provincial Archives in electronic form at this time.

Regardless of which approach ministries use for managing e-mail messages, users must have a clear understanding of how to decide which e-mail messages they need to retain and how to store them. Filing systems, whether for paper or electronic records, need to be kept up-to-date, and procedures for disposing of records appropriately must be established and followed.

Security of systems and e-mail

Information technology systems, including e-mail, must conform to the Government of Alberta Information Technology Security Policy.

Most e-mail systems are designed for easy communications, while employing some standard security measures such as access controls, authentication of users, confidential mailboxes and activity reports.

There are several security risks associated with using e-mail to conduct business. These risks include

- the downloading of viruses that infect computer systems;
- the simple misdirection of e-mail to unintended recipients;
- the non-delivery of e-mail; or
- redirection of government e-mail to non-government mail systems (for example, home computers or other public access systems).

Ministries should take all appropriate physical and technical security measures to protect the information transmitted over e-mail.

Practices and guidelines should help users understand the nature of security related to e-mail. Security and back-up measures that are in place for the e-mail system in order to protect records from alteration, loss, or inappropriate destruction may include the following:

- **Virus Protection:** Users should be aware of the virus protection that is provided automatically and of the risk posed by viruses, including 'trojans' that can open their system's confidential files. The guidelines should also identify practices related to the types of attachments that should not be opened and the virus protection that is required for home computers that are used for ministry work.
- **Back-up Procedures**: Back-up measures are usually established for e-mail systems for security and disaster recovery purposes. These permit information to be restored should the system crash or if the e-mail system is damaged in some other way. Users should understand the nature of and timing of ministry back-up procedures. Users should also understand how long back-up versions of e-mail are retained.
- **Password Protection**: Passwords or other access controls protect e-mail systems and workstations from unauthorized users. The guidelines should give users basic advice on choosing and updating passwords and how to protect their passwords.
- **Message Protection and Authentication Controls**: Employees should be made aware that e-mail communication can be forwarded, intercepted, printed and stored by others, thus there is no way to guarantee privacy. Message protection and authentication prevent others from changing an e-mail message once it has been received by at least one recipient. The controls require users to send a new message with new transmission and receipt data if they wish to change the content of a message. The use of these control measures should be explained to users as a vital support within the system for the authentication and version control over e-mail.
- **Security Labels**: Protocols for the use of security labels such as "confidential," should be explained to users. Such labels can be attached to e-mail by senders to alert recipients about special privacy or security handling requirements. The guidelines should describe the circumstances where these measures may be employed and the practices to be used in particular circumstances.
- **System and 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 e-mail system or on a network. Such practices

should be used where business needs make them appropriate and users should be informed about them.

- **Encryption**: Users should be made aware of the encryption methods available to them, and the ministry practices for using encryption. If encryption methods are available, appropriate safeguards to recover encrypted messages must be in place. Employees should be told very clearly that the communications system is not encrypted by default.

Ensuring the reliability and authenticity of e-mail

Reliability, authenticity, and integrity are the characteristics used to describe trustworthy records from a legal and records management perspective. Ministries need to consider these characteristics when planning and implementing practices related to the management of e-mail.

If e-mail might be used as evidence in court, for claims, or in others types of legal proceedings, it is essential to demonstrate the reliability, authenticity and integrity of the record.

- **Reliability**. A reliable record is one in which the content can be trusted as a full and accurate representation of the transaction, activity or fact to which it attests, and can be depended upon in the course of subsequent transactions.
- **Authenticity**. An authentic record is one that can be proven to be genuine and to have been created or sent by the person who claims to have created and sent it.
- **Integrity**. The integrity of a record refers to it being complete and unaltered.

To ensure the reliability, authenticity and integrity of messages created or received through e-mail systems, ministry procedures should ensure that

- information identifying the creator, receiver, date, and transmission of the message is maintained;
- the e-mail cannot be altered and, if it is forwarded, the original message cannot be changed.
- an audit trail is recorded;
- if electronic signatures are used, they are provided via approved methods, can be verified and are retained as part of the message, as prescribed in the *Electronic Transactions Act*; and
- rules concerning the authenticity and integrity of electronic records are followed, as set out in the *Alberta Evidence Act*.

Ministry practices should be explicit in providing users with guidance on maintaining the content, structure and context of electronic messages.

Complying with FOIP

Any records in the e-mail system are in the custody or under the control of the ministry and, thus, may be included in a request for information under the *Freedom of Information and Protection of Privacy Act*.

FOIP Bulletin Number 12:"E-Mail: Access and Privacy Considerations" can assist ministries in complying with their obligations under the FOIP Act by highlighting the access and privacy protection issues raised by e-mail.

Employees may be asked to search their e-mail to locate information pertinent to an access request. Information that has already been permanently destroyed under an approved records retention and disposition schedule need not be recovered (e.g. back-up tapes will likely not need to be searched).

The same rules apply to e-mail as to other types of information subject to an access request. No information that may be responsive to a FOIP request may be destroyed after the request has been received until the request has been completed and all applicable review periods have expired. This remains the case even where approved records retention and disposition schedules are in place.

The Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile prohibits the external transmission of personal information via e-mail unless

- personal identifiers have been removed; or
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other acceptable means are used by both the sender and recipient to ensure confidentiality and protection of privacy are maintained.

The ministry's practices should indicate methods that staff can use when sensitive personal information must be sent by e-mail. For example, one method would be to ensure the personal information is contained in an attachment and to password protect the attachment.

Monitoring of e-mail

E-mail systems are routinely monitored for capacity and storage to maintain the efficiency of the system. However, the ministry's guidelines should clearly state under what conditions the system administrator and other authorized individuals will monitor an individual's e-mail messages. These conditions should take into account the following factors:

- users of the system may have some expectation of privacy;
- general monitoring of e-mail communications for unspecified purposes should not be allowed;
- there will be no secret monitoring or search, except as permitted by law; and
- all collection, use and disclosure of personal information involving an e-mail system will be done in accordance with the legal requirements of the *Freedom of Information and Protection of Privacy Act*.

If monitoring takes place, system users should be asked to help to design the process, be fully informed as to the tools used and how they will operate, and how the collected information will be used.

Usage practices

Ministries should also establish common usage practices that support the effective and efficient use of e-mail. The usage practices will vary depending on the nature of the business and the organization, but could include the following:

- Establish who is responsible for managing the e-mail record. This is especially important in work groups within a ministry or in other instances where many people might receive the same e-mail message. Records should be managed as they relate to business activities of the ministry and as they relate to the activities of the business unit with primary responsibility. This can avoid duplication of effort.
- Ensure that when dealing with sensitive information, the e-mail is sent to the correct recipient(s). This is particularly important if the e-mail is being sent to a long distribution list. Some common practices related to this issue include
    - ensuring the e-mail 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 the entire list; and
    - not forwarding another author's e-mail message to a discussion group, Listserv™, newsgroup or posting it on an electronic bulletin board without the author's permission.
- Review the hidden text in electronic documents before attaching them to e-mail messages to ensure that incorrect or inappropriate information is not conveyed to the recipient. This is especially important if comments have been added or the change-tracking feature has been used to track revisions to the document. The document properties should also be checked to ensure that they reflect the correct title, author and other details.
- Implement practices to reduce the "clutter" or volume of e-mail traffic on a system. Some usage practices for employees in this regard are
    - using "reply to all" only when appropriate (i.e. when all recipients of the original message need to see the reply); and
    - if possible, posting attachments in one location (e.g. an Intranet, shared drive or public e-mail folder where everyone has access to the drive) and "point to them."
- Give guidance on how to handle junk mail (also known as spam), chain letters, e-mail scams and unsolicited attachments. For example, many organizations warn staff not to respond to junk mail as this can verify the e-mail address to the sender making it more valuable and resulting in more junk mail.

Roles and responsibilities for managing e-mail

A section of each ministry's guidelines should address the responsibilities of business managers, program staff, support staff, network administrators, technical staff, and records management staff in regard to the various aspects of managing e-mail.

Business managers should be responsible for ensuring that the records related to their functions, activities and transactions are managed appropriately. It is their responsibility to ensure staff are actually managing e-mail appropriately.

All **users** should be charged with specific responsibilities. These would generally be comprised of the following:

- retaining records of government business, in the format and media required by the ministry and organized in a way that makes them accessible to those authorized to know the contents;
- removing records of personal business and transitory records from e-mail systems on a regular basis;
- protecting all e-mail records from unauthorized disclosure to third parties and from inadvertent loss or destruction;
- protecting personal information in e-mail messages according to the requirements of the *Freedom of Information and Protection of Privacy Act* and government policy; and
- disposing of e-mail records according to approved records retention and disposition schedules.

Systems administrators, FOIP Coordinators, records management and program staff should cooperate in establishing information management rules and best practices for the e-mail system.

Training

Orientation and training should be offered to employees on the general use of e-mail and policies specific to e-mail. Users should have access to training, as needed, to ensure they understand the characteristics of e-mail, the features provided in their work setting and their responsibilities related to the management of e-mail.

The following types of training will be needed by staff:

- training on the basic, intermediate and advanced functions of the ministry's e-mail system;
- training on identifying transitory records (a model training program was instituted at the ministries of Environment, Sustainable Resource Development, and Energy – other ministries may also offer training);
- training on how to manage e-mail records in a manner that is consistent with the ministry's preferred method of managing electronic records (e.g. in electronic records and document management systems, in shared drives, within the e-mail system, in print); and
- training on the ministry's practices (e.g. usage and security).

Managing Information @ Work awareness session materials have been developed to assist ministries.

4.
MANAGING E-MAIL AT THE DESKTOP

Most people complain about the number of e-mail messages they receive each day and the time devoted to processing them. While this feeling of "information overload" has many causes – such as receiving unnecessary junk mail – one cause is related to the fact that we all have to manage these messages.

> Recent studies suggest that employees spend an average of 49 minutes a day managing e-mail, with almost a quarter spending more than an hour a day managing e-mail. (Gartner, 2001)

If you set up some basic procedures, you can reduce the anxiety of dealing with this responsibility. Here are some practices that individual users can put in place to help manage e-mail at the desktop.

Follow your ministry's security and usage practices

Learn about the security and usage practices that have been set up in your ministry. These practices will cover things like

- how the ministry integrates the management of e-mail records with other records;
- tools such as passwords, back-ups, virus protection and encryption to protect the integrity of electronic mail and to protect confidential or sensitive information;
- compliance with freedom of information and privacy requirements; and
- other advice on how to manage e-mail effectively.

Manage e-mail messages as records

It is every employee's responsibility to manage e-mail messages as records. Records are evidence of business activities and transactions and can be in any medium or format, including electronic media such as e-mail.

There are two categories of records: official and transitory. Official records are those that

- are required to maintain business operations;
- document and provide evidence of business transactions;
- protect the rights of citizens and the government;
- provide evidence of compliance with accountability or other business requirements; or
- will have some future business, legal, research or archival value to the government and people of Alberta.

Official records should be organized and filed in ministry filing systems. Some examples of such records include

- policies and directives;

- correspondence related to the business of the ministry;
- work schedules and assignments;
- agendas and minutes of meetings;
- any record that initiates, authorizes or completes a business transaction; and
- final reports or recommendations.

If the e-mail message documents government business, you must manage it in the same way you would manage records in other media such as paper. Follow your ministry's guidelines for managing electronic mail and records – in folders within e-mail, within broader electronic records and document management systems, or by printing off records to include in the manual system. If you are unclear about the procedures, talk to the records management contact or Senior Records Officer in your ministry.

Regularly delete transitory records

A significant number of e-mail messages are transitory or temporary in nature and do not merit long-term retention. Transitory messages can be routinely deleted from your e-mail system.

The government's Official and Transitory Records: A Guide for Government of Alberta Employees includes a helpful description of the range of transitory records. The categories that relate most closely to e-mail are:

IMPORTANT

There is personal judgment involved in deciding what is a transitory record.

The categories described here are examples.

Sometimes what appears as a simple message actually documents an administrative or operational activity.

If you are not sure, ask the Senior Records Officer in your ministry.

- **Information of Short-Term Value**: This category includes records containing information that is either of no importance or value to a ministry, or that is only of immediate or short-term use and has no future value. This category would include personal messages and announcements that are not related to the conduct of ministry business. These messages should be routinely deleted as transitory records.

Examples: Simple messages which are the equivalent of a telephone message slip asking a person to contact another person or to coordinate a lunch appointment with a friend; announcements of social events such as retirement parties or a notice concerning holiday celebrations; shared calendars and daily diaries and information notes of little consequence such as sending a birthday or congratulatory message to a relative.

- **Duplicate Documents**: Duplicate documents are exact reproductions of records where
  - nothing has been added, changed or deleted;
  - the documents were created and used only for convenience or reference purposes; and

- the master version of the document has been filed in a records or information system and is scheduled for disposition along with that record series.

Examples: Some examples of duplicate documents in e-mail systems might be a finished document sent to all employees to inform them of a new departmental program, activity or approach to an issue. It could also be a "cc" copy of a message or document sent to the employee.

- **Draft Documents and Working Materials**: These documents are records that contain information that has been used to create a master record. Once a master record has been produced and incorporated into a records or information system, most draft and working materials become transitory records. However, if the draft material documents a policy development process or the basis for assuming an administrative or operational approach, the documents should be incorporated into the records or information system and scheduled as part of a records series.

IMPORTANT

Drafts and working materials should be **retained** if they were used in the preparation of:

- legislation;
- legal documents;
- policies, standards, guidelines and procedures;
- audit reports; or are
- accounting working papers.

Examples: Drafts of correspondence; reports and other documents; calculations; research materials; rough notes; editing and formatting notes; and rough documents.

Identify who is responsible for a message

Some messages, especially messages that are sent to an internal group, may not need to be managed by everyone in the group. For example, if you have a committee or task force working on project, try to decide early on in the process who is going to be responsible for managing the e-mail records of the group. This might save everyone time!

Manage all your e-mail folders

Make sure you manage all your folders – Inbox, Sent Items, Deleted Items, Drafts, and other folders you have created within your e-mail system. While most people manage their "inbox," many forget to manage the records in their "sent items" folder. Since you initiated the messages in your "sent items" folder, it is probably the most important folder to manage and the one most ignored by users.

Empty your "deleted items" folder regularly. If you don't empty the "discarded items" folder, the records remain on the system and are in the custody and under the control of your ministry and remain accessible under the *Freedom of Information and Protection of Privacy Act*. Also, any personal messages you deleted will remain on the system if you don't empty the "deleted items" folder.

Try managing information as it comes in, so you don't have to spend long hours doing it at the end of the week or when you receive a message from the systems administrator informing you that you have exceeded your allocated amount of space on the e-mail server.

Make your e-mail effective

Remember that your colleagues have to manage their e-mail too. Making effective use of e-mail can help everyone better manage information. A tool you can use to help you make your e-mail effective is Ten Ways to Make E-Mail Effective (Appendix 2).

Use caution when opening 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 e-mail users open attachments without question, or even have their software open all attachments upon receiving them.

Security precautions for handling attachments include avoiding opening unsolicited attachments, regardless of the sender. As well,

- check with the sender about the authenticity of an attachment before opening it;
- save the attachment to your computer or disc and then scan it with anti-virus software;
- turn off the e-mail function that automatically opens attachments.

E-mail while out of the office

Using the *out of the office* auto reply is a handy way to alert clients and staff of your absence, but there are security aspects involved.

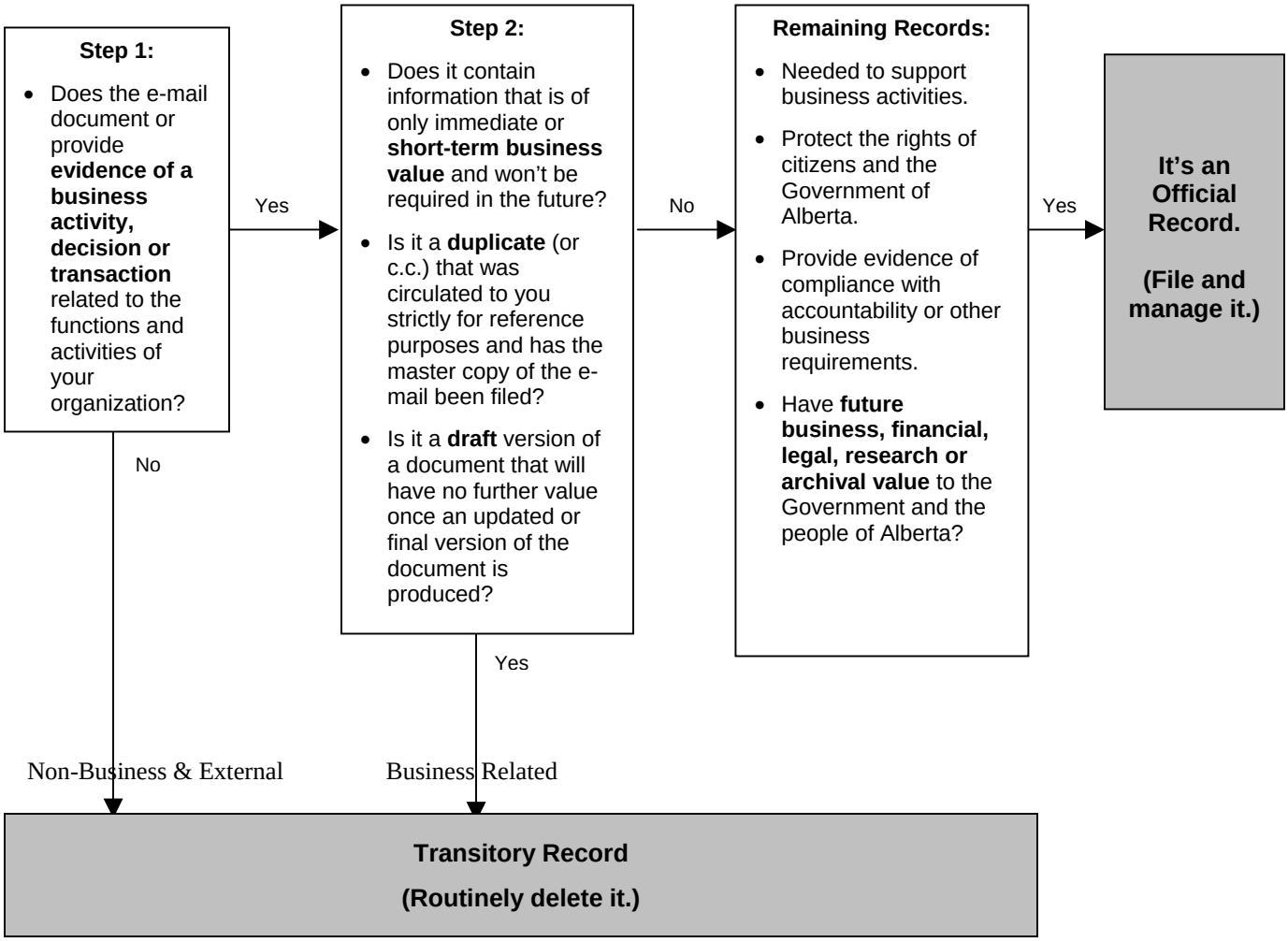
- Alerting people to your absence allows for knowledge of your whereabouts that you might not want known. For example, "I will be out of the office for 2 weeks while in Europe" is valuable information for home invaders.
- If your e-mail uses the reply-all function and you receive department wide e-mail, your *out of the office* reply will spam your own department.
- Consider the appropriateness of using the auto-forwarding feature while you are away and forwarding official government e-mail to your own personal e-mail.

A practical method of keeping up with your e-mail is to appoint a designated person to access your e-mail while you are gone. This can be done by setting up your inbox properties without giving away your password.

APPENDIX 1: IDENTIFYING AND DELETING TRANSITORY RECORDS

What information do I need to keep?

You need to distinguish between official records that document and provide evidence of government business transactions, and will have future value, and transitory records that are temporary in nature and have little administrative or operational value. The diagram below can help you identify records that are considered "transitory" and, thus, can be deleted.



The government's Official and Transitory Records: A Guide for Government of Alberta Employees includes a helpful description of the range of transitory records.

APPENDIX 2:
TEN WAYS TO MAKE E-MAIL EFFECTIVE

Everyone seems to complain about the volume of e-mail they receive. Here are 10 tips to make your e-mail effective and easier to process for the recipient of your message. The general guideline is, "use common sense when creating and sending e-mail!"

1. **Keep the message as short as possible.**

   While there is no specific size limit, long and complex messages are hard to read, waste time and may be ignored. A message should be as short as possible while providing the recipients the information they need. One subject per message is a good general rule.

2. **Use a short, descriptive subject line.**

   Put yourself in the place of the reader when selecting the wording of the subject line. Will the subject line help them sort the message and prepare them for what they are about to read?

3. **Clearly state the primary audience.**

   State the primary audience at the beginning of the message.

   For example, if the message is to unit supervisors, but all staff are copied (e.g. "cc"), then stating the intended audience will help others understand why they are receiving the message. In this case, "Attention: Unit Supervisors" at the top of the message will help.

4. **Clearly state the importance or urgency of your message.**

   Put this information at the beginning of the message or use features built into e-mail systems such as MS Outlook.

5. **Put an "action requested" line at the top of the message.**

   For example:
   Action: Reply by 4:30 p.m., January 10, 2004

6. **Avoid jargon and acronyms.**

   This is particularly important when sending e-mail to an audience that may not be familiar with jargon and acronyms commonly used in your work group. If using acronyms in the message to keep the message short, spell out the full term the first time followed by the acronym in parentheses.

7. Format messages for easy reading.

Keep the layout and structure of the e-mail simple and avoid complex formatting and graphics.

Also, when people read electronically, they tend to scan more than when they read printed information. So, it's a good idea to keep your paragraphs short to facilitate scanning.

8. Avoid "reply to all."

Be careful using "Reply-to-All" when responding to a message, particularly if the original message was sent to a large audience. "Reply-to-All" is only needed where the reply is important and relevant to the *majority* of recipients of the original message.

9. Do not send large attachments. Post once and point.

Although your dedicated connection to the Internet may be quite fast, a recipient outside of your ministry may have a slow connection. Attachments should only be sent to people who have an active need for the majority of information in the attachments, and if the information is too much to include in the body of a message. If the information is only of possible interest, it is better to post the information to an area accessible to the appropriate audience, such as on an Internet site available to the public or on an Internet site where access is restricted to specific individuals (e.g. an extranet).

Generally speaking, avoid sending a file that is over 1MB in size, unless you know that the recipient has a fast connection or, if it is very important and e-mail is the only way to get the information there quickly. If the file is very large, you could compress it before sending it, or deliver it in another way (e.g. on an Internet or Intranet site or on CD-ROM).

Always review the hidden text in electronic documents before attaching them to e-mail messages to avoid conveying incorrect or inappropriate information. This is especially important if comments have been added or the change-tracking feature has been used to track revisions to document.

If you use the change-tracking feature in Microsoft Word or other software, it is highly recommended that you also use the "Accept Changes" function before releasing your document to the public (e.g. e-mailing it to stakeholders or posting it to a web site). If you fail to "Accept Changes," Word keeps your earlier drafts, which might contain sensitive or incorrect information, within the document. Anyone can view this information by turning on the "Highlight Changes" feature in Word.

You should also check the document properties to ensure that they reflect the correct title, author and other details about your document.

10. Use distribution lists sparingly.

Use the right distribution list for each message. When there are many lists it is easy to select the wrong one.

Before you use a list, check to see who is on it and verify its accuracy. When creating distribution lists, limit each list to those individuals who are likely to need the same type of information. This may be based on organization (such as all people in a unit), function (all managers and directors) or specific interest (a temporary work group for a project).

Keep the list up-to-date. People often change jobs and e-mail addresses. This is particularly important for people outside the ministry who you contact infrequently.

Also remember to keep your e-mail professional in both content and tone. Remember, it could subject to a FOIP request.

APPENDIX 3:
SAMPLE MINISTRY GUIDELINES AND PRACTICES

This section contains an example of ministry guidelines and practices related to e-mail. Additional or alternative guidelines and practices could be added based on the business needs of the ministry.

Topic	Guidelines and Practices
Integrating e-mail records with other records management practices	The normal practice for managing e-mail records in the ministry will be to integrate them into existing folders on shared drives that parallel our traditional paper records management classification structure. At both the corporate and business level, folders will be established in the electronic shared drive file structure that parallel the ministry's records classification system for paper records and are linked to approved records retention and disposition schedules. The Senior Records Officer and IT services will provide advice on the "set up" of public folders and linkage to schedules. Drafts, duplicates and reference documents will not be filed in directories containing completed versions and official records. Until such folders are established, it is the policy of the ministry to print and file all e-mail (except transitory and personal). Each business unit must establish responsibility for managing messages stored in electronic form according to approved records management policies and records retention and disposition schedules. Only authorized staff will have authority to delete records from corporate and business level folders, using documented, auditable procedures.
Protecting the security of the system and messages	**Protection against viruses** Virus protection can occur at three levels: when the e-mail message first enters the government's e-mail system, when it reaches the ministry's network, and at the desktop level. Given the risk of viruses in today's environment, employees should • not open attachments that are from unknown senders or that have an ".exe ," ".vbs," or ".bat" extension; and • regularly update the virus protection on the desktop. This can be done by….[insert details]

Topic	Guidelines and Practices
	Back-up Procedures The ministry performs "back-up" procedures every night. Electronic files (including e-mails) that are created/received AND deleted the same day will not be backed up on the system, and thus are irretrievable through back-up procedures. **Password Protection** The use of the password is a shared responsibility of individual employees and IT administrators. You should: • Not share passwords with other employees. To do so exposes you to responsibility for actions that others may take using the password and your ID. • Change your password regularly (every three months) when prompted by the system. • Select a password for your screen saver (that way, if you are away from your desk, others cannot access confidential information in your files). Alternatively you can "lock" your computer if your operating system provides this feature (e.g. available in Windows 2000). **Message Protection and Authentication Controls** E-mail records are the property of the Government of Alberta. These records should NOT be left on machines where they may be accessible by others. Therefore, do not download your e-mail to any non-government machine (except your home computer). If you download e-mail at home, you MUST delete messages as you review them and ensure that no Government of Alberta messages remain on your home system. Access to the ministry's e-mail from non-government machines should generally be avoided. Attachments may be left on machines in libraries, kiosks and other places without you realizing it. Remote access to e-mail from outside of the ministry should be done only with security protocols that allow for two-level authentication. Do NOT forward e-mail from the Government of Alberta account to a personal account such as hotmail.com. Apply the "confidential" flag on outgoing messages where appropriate to alert recipients about special privacy or security handling requirements.

Topic	Guidelines and Practices
	Encryption The ministry does not have a standard for encryption of messages. Before you attempt to encrypt messages, please consult IT services to ensure encrypted messages are accessible if required in the future.
Compliance with FOIP legislation	**Access** All records, including e-mail records, in the custody or under the control of the ministry may be subject to access by the public on request. If the ministry receives a request to access information, all employees may be asked to search their personal e-mail folders, in addition to public folders and shared drives, to comply with the request. It is unlawful to knowingly delete any message related to a request for access to information until the request has been satisfied and all periods of appeal have been exhausted. **Privacy** Personal information contained in e-mail must be protected. Under normal circumstances, sensitive personal information should not be sent though e-mail so that privacy of the information is protected. If you must send personal information through e-mail, you should • ensure that the personal information is contained in an attachment; • password protect the attachment; • notify the recipient of the password for the attachment using a different method of communication (e.g. telephone); and • request a confirmation of receipt from the recipient of the message.
Monitoring e-mail	The ministry will regularly monitor the e-mail system for potential threats to security and the functioning of the system. The normal practice of the ministry is not to monitor individual e-mail messages for unspecified purposes. However, we may investigate the content of individual e-mail messages • if we suspect a violation of any policy, law, the Official Oath of Office or the Code of Conduct and Ethics for the Public Service of Alberta agreed to by all employees. Potential violations might include safety violations, illegal activity, misuse of

Topic	Guidelines and Practices
	corporate resources, racial discrimination, and sexual harassment. • for the purpose of evaluating an employee's performance or activities. Employees will be consulted before any monitoring is done. • if it is necessary for another staff member to access an employee's work-related e-mail messages when the employee is working out of the office, on vacation, or is away due to illness. Employees will be asked for access to their e-mail prior to their absence from the office whenever possible.
Usage practices for e-mail	E-mail can make communication with colleagues and clients easier. Employees are encouraged to make use of this vehicle. However, too much of a good thing can create problems. To make sure the system continues to run smoothly, the following is suggested: • Use "reply to all" only if all recipients of the original message need to receive your reply. If not, reply only to the sender of the original message. • Use the ministry Intranet and shared drives, or the ministry's Internet or secure extranet site, as much as possible to "post messages" that others can view. This keeps the number of attachments to a minimum. • If sending attachments outside of the ministry, ensure that the receiver can receive and read the attachment, and check for any hidden text that may contain incorrect or sensitive information. For example, delete inappropriate comments and review the document properties to verify the title, author and other details. If the change-tracking feature in Microsoft Word or other software has been used, you must also use the "Accept Changes" function, otherwise the receiver will be able to view earlier drafts of your document by turning on the "Highlight Changes" feature in Word. • Do NOT respond to junk mail, spam or other types of unsolicited messages. This includes chain letters sent to you by someone you know. If you respond to these messages, the information can be used to generate more "junk" mail messages. The best advice is: "ignore them and delete them without reading them." • Do NOT send jokes or other non-work related programs as attachments as they use up considerable system resources.

Topic	Guidelines and Practices
Roles and responsibilities for managing e-mail	Individual managers in the ministry will be held accountable for the management of e-mail records by their employees. Managers must ensure that employees have training to be able to properly manage their e-mail records. Managers must also establish a regular review with employees to ensure that e-mail records as well as other records are being managed according to ministry guidelines and practices. The management of e-mail records, along with other records management responsibilities will form part of each manager's performance evaluation. All users of the ministry's e-mail system have the following responsibilities: • Users should remove personal and transitory records from personal mail boxes on a regular basis. • All other records (i.e. not personal or transitory) will be stored in the appropriate folder, format and media required by the ministry and organized in a way that makes them accessible to those authorized to know the contents. • The disposition of e-mail records must be done according to approved current records retention and disposition schedules.
Other	All electronic communication generated, stored or handled by the government servers/microcomputers (including back-ups) is the property of the Government of Alberta. Any personal messages (not about government business) should be routinely deleted from the systems.

APPENDIX 4: GLOSSARY

Authentication Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).

Bulletin Board System (BBS) Before the Web took over the world, computer hobbyists and companies often communicated with other techies via electronic bulletin board systems, or BBSs.

The Web has largely replaced BBSs for most purposes, though some individuals and companies still maintain their systems or even connect them directly to the Web.

E-Mail Electronic Mail — are messages sent from one person to another via computer. They are usually text, but can include attached files, HTML codes, voicemail messages, etc.

E-mail can also be sent automatically to a large number of addresses (see also Mailing List).

E-Mail Scams There are a wide variety of scams being perpetrated on the Internet using email.

One type is the false virus warning or hoax. These often take the form of a warning not to open an e-mail with a certain subject line, and asking you to pass on the warning. These are almost always scams and are designed to waste resources by resulting in millions of copies of the warning using bandwidth and filling up e-mail storage. Most antivirus web sites have pages listing hoaxes (for example: http://securityresponse.symantec.com/avcenter/hoax.html). People should always make sure an e-mail warning is not a hoax before forwarding it.

Another common scam is the “get rich quick” scam or requests for donations of money.

Encryption Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key.

HTML HyperText Markup Language — The language used to create Hypertext documents for use on the World Wide Web. HTML files are meant to be viewed using a World Wide Web Client Program or browser. HTML is also an alternative for sending formatted text messages in some e-mail systems.

Listserv™ The most common kind of Internet mailing list. Listserv® is a registered trademark of L-Soft International, Inc.

Mailing List A system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the mailing list. In this way, people who have many different kinds of e-mail access can participate in discussions together.

Newsgroup A worldwide system of discussion groups, with comments passed among thousands of machines.

The system, also called USENET, is decentralized, with over 10,000 discussion areas, called newsgroups.

Official Record An official record is a record that has some future administrative, financial, legal, research or historical value to the government and is therefore retained and filed in a recordkeeping system.

Personal Information Personal information is defined in section 1(n) of the FOIP Act as recorded information about an identifiable individual, including but not limited to:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information, or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

Record Record is defined in section 1(q) of the FOIP Act as "a record of information in any form, and includes notes, images, and audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records."

Recordkeeping Manual or computerized information system which captures, manages and provides access to records over time.

Records Retention and Disposition Schedule Legal documents that describe different series of government records, establish how long they must be retained and what their final disposition will be, either destruction or archival preservation.

Transitory Record	A transitory record is a record containing information of temporary value which does not have future administrative, financial, legal, research, or historical value to the government. This may include duplicate records, draft documents, working materials, external publications, blank forms, and temporary notes provided that they do not have long-term value.
Trojan Horse	In computers, a Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming in such a way that it can get control and do its chosen form of damage, such as allowing someone else to access your computer over the Internet. See also Virus.
Virus	A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Most viruses can also replicate themselves and are distributed by disks or over networks and the Internet. All computer viruses are manmade. Even a simple virus is dangerous because it can use up resources and even damage or delete all information on your system. See also Trojan Horse.

APPENDIX 5: Resources

Looking for more information related to the management of e-mail? The sources listed below can help.

Note: Several documents listed in this appendix are available on the Shared Repository (SHARP) (http://www.sharp.gov.ab.ca). This site is accessible to Government of Alberta employees (name@gov.ab.ca) and also to extended stakeholders (i.e. agencies, boards and commissions), consultants contracting with the Government of Alberta and employees of other governments who are registered users of the SHARP web site.

E-mail and Information Management

Office of the Corporate Chief Information Officer, and Alberta Government Services, Information Management Branch.
Government of Alberta Information Management Framework.
http://www.im.gov.ab.ca

E-mail and IT Security

Office of the Corporate Chief Information Officer.
Using E-mail: Detailed Risks and Controls.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=4442

Office of the Corporate Chief Information Officer.
Using E-mail: Managing the Risks.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=4441

Office of the Corporate Chief Information Officer.
Government of Alberta Information Technology Security Policy.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=3078

E-mail and Public Access

Alberta Government Services, Access and Privacy Branch.
FOIP Bulletin Number 12: "E-Mail: Access and Privacy Considerations."
http://www.gov.ab.ca/foip/guidelines_practices/bulletins/bulletin12.cfm

E-mail Use

Office of the Corporate Chief Information Officer.
Government of Alberta Internet and E-mail Use Policy
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=2007

Commonwealth Films. **The Plugged-in Mailbox: E-mail Uses and Misuses.** (Video and Guide). http://www.commonwealthfilms.com/s/1_10_39.asp

Employee Code of Conduct

Alberta Personnel Administration Office.
Code of Conduct and Ethics for the Public Service of Alberta.
http://www.pao.gov.ab.ca/legreg/code

Legislation – available on the Queen's Printer at http://www.qp.gov.ab.ca

- *Alberta Evidence Act*
- *Electronic Transactions Act*
- *Freedom of Information and Protection of Privacy Act*
- *Health Information Act*
- *Historical Resources Act*
- *Government Emergency Planning Regulation*
- *Records Management Regulation*

Managing E-mail

National Archives of Canada.
E-mail Management in the Government of Canada.
http://www.collectionscanada.ca/information-management/060404_e.html

ARMA International (Association for Information Management Professionals) Lenexa, Kansas

- **E-Mail Rules**: **A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communications.** Nancy Flynn and Randolf Kahn, 2003 ISBN: 0-8144-8188-9.
  http://www.arma.org/bookstore/productdetail.cfm?ProductID=1383
- **Guideline for Managing E-mail**, ARMA International, 2000. ISBN: 0-933-887-91-4. http://www.arma.org/bookstore/productdetail.cfm?ProductID=1045
- **Legal Obstacles to E-Mail Message Destruction**, ARMA International Educational Foundation, 2003.
  http://www.armaedfoundation.org/images/LegalObstaclesToEmailDestructionV634.pdf.
- **Managing Your E-Mail Thinking Outside the Inbox** by Christina Cavanagh 2003 ISBN: 0-471-45738-8.
  http://risk-management.argospress.com/book-0471457388.htm
- **E-mail, Voicemail and Instant Messaging: A Legal Perspective.** (IMJ Read & Learn Course)
  http://www.arma.org/learningcenter/onlinecourses/courselising.cfm?CourseID-20

- **Requirements for Managing Electronic Messages as Records (ANSI/ARMA 9-2004)** ARMA International ISBN 1-931786-22-4. http://www.arma.org/bookstore/productdetail.cfm?ProductID=1499

- Natural Resources Canada. **Guidelines on Managing Electronic Mail Messages**, 2004. http://www.nrcan.gc.ca/em-ce/email-e.htm

Protecting Personal Information and Privacy

Office of the Corporate Chief Information Officer.
Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=3546

Alberta Government Services, Access and Privacy Branch.

- **FOIP Guidelines and Practices.**
  http://www.gov.ab.ca/foip/guidelines_practices
- **FOIP Bulletin Number 12: "E-Mail: Access and Privacy Considerations."**
  http://www.gov.ab.ca/foip/guidelines_practices/bulletins/bulletin12.cfm

Records Management

Alberta Government Services, Information Management Branch.

- **Official and Transitory Records: A Guide for Government of Alberta Employees**.
  http://www.im.gov.ab.ca/publications/pdf/OfficialTransitoryRecordsGuide.pdf

Web Sites

The following web sites offer guidelines, forms, books, newsletters, training tools, workshops, discussion forums, software and other resources relating to the development, implementation and enforcement of e-mail policies.

- **Treasury Board of Canada Secretariat Information Management Resource Center: E-mail Management.**
  http://www.cio-dpi.gc.ca/im-gi/references/email-courrier/email-courrier_e.asp
- **Email-Policy.com**
  http://www.email-policy.com
- **ePolicy Institute**
  http://www.epolicyinstitute.com