Guidelines for Managing Emails

Email has become one of the main forms of business communication. Business decisions, key communications and important information are regularly shared by email. Yet, people often do not think of emails as records or they view emails as having short term or no business value and therefore not required to be kept.

In light of the vast quantities of email sent and received daily by an organization, email management is not just a records management issue but is also a necessary business process. Improper email management can increase organizational risks and costs from:

- An inability to provide evidence of an action taken or decision made
- A loss of critical records and corporate memory
- Inefficient and ineffective search and retrieval of records, whether in response to an access to information request or litigation hold, or for general corporate use
- Protecting, storing and migrating emails that are not required for business purposes

In addition, the management of emails has become the subject of investigation reports and orders issued by information and privacy commissioners across Canada.[1] Some of the identified issues and risks associated with the mismanagement of email include:

- Increased instances of no records existing
- No clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access to information request
- Lack of records management training including the identification of transitory and official records and the process for retaining and disposing of records
- Emails not being captured in the organization's records management system for official records

[1] For example, Office of the Information and Privacy Commissioner of Alberta, *Investigation Report F2019-IR-01: Investigation of the management and storage of email by the Government of Alberta*; Office of the Information and Privacy Commissioner for British Columbia, *Investigation Report F15-03: Access Denied: Record Retention and Disposal Practices of the Government of British Columbia*; and Office of the Information and Privacy Commissioner of Ontario, *Deleting Accountability: Records Management Practice of Political Staff – A Special Investigation Report* (2013), and Order PO-3304.

Office of the Information and Privacy Commissioner of Alberta

March 2019

The Office of the Information and Privacy Commissioner of Alberta (OIPC) is issuing this high-level guidance document to assist public bodies, health custodians and private sector organizations and their staff in understanding that emails are records and should be managed in accordance with records management principles and the requirements of Alberta's access to information and privacy legislation.

Although the guidance provided in this document is directed at managing emails, the general principles may assist in managing records in other formats. **Readers should consult the records management and information technology practices, policies and requirements of their own public body, custodian or organization for details about how emails, and other records, are managed within their environment.**

Note: Unless otherwise indicated, the term "organization" in this document encompasses public bodies, health custodians and private sector organizations, for ease of reference.

Emails Are Records

In simple terms, a record is information that is recorded in any format or medium. Records can be paper, photographs, videotapes, audio recordings, films, maps, photographs, x-rays, electronic documents and spreadsheets, electronic messages, and other media.

An email meets the definition of a record – an email is a recorded message created, sent or received within an electronic system. Emails are also defined as a "record" under Alberta's three access and privacy statutes:

- *Freedom of Information and Protection of Privacy Act* (FOIP Act)[2]

  Section 1(q): "record" means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books,[3] documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any matter, but does not include software or any mechanism that produces records.

- *Health Information Act* (HIA)[4]

  Section 1(1)(t): "record" means a record of health information in any form and includes notes, images, 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 matter, but does not include software or any mechanism that produces records.

---

2 RSA 2000, c. F-25. Retrieved from www.qp.alberta.ca/documents/Acts/F25.pdf.

3 Although the definition of "record" includes books, the FOIP Act does not apply to "published works collected by a library of a public body in accordance with the library's acquisition of materials policy" (section 4(1)(j.1)).

4 RSA 2000, c. H-5. Retrieved from www.qp.alberta.ca/documents/Acts/H05.pdf.

- *Personal Information Protection Act* (PIPA)[5]

  Section 1(1)(m): "record" means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or any other form, but does not include a computer program or other mechanism that can produce a record.

Therefore, public bodies, custodians and organizations must apply the access and privacy provisions of these Acts to the emails in their custody or under their control.

Implement Effective Records Management Practices

As a record, emails should be captured and governed by the organization's corporate records management policies and practices.

Effective and efficient records management practices ensure that evidence of business transactions and decisions is created, captured, managed and made accessible to those who need it, for as long as it is required,[6] regardless of the medium or format of the record.

Implementing good records management practices also assists organizations with responding accurately and completely to an access to information request and within the required timeframe. Records can be prevented from being lost or inappropriately deleted and search times and associated fees for finding responsive records can be reduced. Searching for responsive records is more difficult when records are stored in locations other than the organization's designated records management system (e.g. stored in an employee's email mailbox, computer hard drive or office drawer where they are accessible only by that employee).

Effective records management practices also:

- Improve transparency and accountability
- Support business operations
- Provide business continuity in the event of a disaster
- Preserve corporate memory
- Assist in litigation
- Safeguard vital information
- Protect the personal/health information privacy of individuals
- Allow correction (or annotation) of personal or health information, when requested

---

[5] SA 2003, c. P-6.5. Retrieved from www.qp.alberta.ca/documents/Acts/P06P5.pdf.

[6] International Organization for Standardization. (2016). *ISO 15489-1: Information and documentation – Records management* (2nd ed.), p. vi. Geneva, Switzerland. Available from www.iso.org/standard/62542.html.

For Government of Alberta departments and agencies, boards, commissions and other bodies listed in Schedule 1 of the FOIP Regulation,[7] the Minister of Service Alberta is required by the *Records Management Regulation*[8] to establish a records management program. The deputy heads of the departments and Schedule 1 bodies must ensure that records in the custody or under the control of their department or body are managed in accordance with the policies, standards and procedures established by the Minister of Service Alberta.[9] Records retention and disposition schedules must also be established and approved.[10]

A corporate email policy should set out the rules for email management that everyone in the organization must follow. The policy should:

- Specify that records sent and received by employees in the course of their employment responsibilities are official records and email messages that have business value must be captured as official records
- Identify which email messages should be captured as official records, who is responsible for capturing the records, and how and when the records are to be retained
- Specify that the organization's records retention and disposition schedule applies to emails that are official records
- Make clear that emails subject to an access to information request or required to be preserved for litigation purposes must not be disposed of even if they are transitory in nature
- Specify that remote or home use of corporate email is still subject to the organization's corporate email management policy or recordkeeping requirements

Official vs. Transitory Records

Not all emails need to be kept. Only those emails that are official records must be retained. Therefore, in order to effectively manage emails, staff must be able to identify what is an official record and what is a transitory record that can be disposed of after it has served its purpose.

Official Records

An **official record** provides documentary evidence of the business transactions, activities and decisions of a public body, custodian or organization. Official records are required for future business, legal or archival purposes. They may be **created** or **received** by an organization and can exist in any media form. It is **content and context** of a record that determines whether it is an official record, not its format or storage medium.

---

7 *Freedom of Information and Protection of Privacy Regulation*, AR 186/2008. Retrieved from www.qp.alberta.ca/documents/Regs/2008_186.pdf.

8 AR 224/2001, section 4. Retrieved from www.qp.alberta.ca/documents/Regs/2001_224.pdf.

9 Ibid, section 9.

10 Ibid, sections 6 and 10.

Official records must be saved and stored securely so that they will be readily available to those who need them and are authorized to access them. Official records must be retained and disposed of in accordance with the records retention and disposition schedule of the organization. Emails that are official records should be covered under the organization's records retention and disposition schedule.

Examples of official records:

- Administrative records typical of any organization (e.g. human resources, finance, office and equipment, contracts, corporate policies and procedures)

- Operational records that relate to the core business activities of the organization

Organizations should implement a "duty to document" policy that requires staff to keep written records of key decisions, actions, deliberations, advice and recommendations arising from the organization's business. A failure to create and retain such records affects the operations of the organization, including its ability to resume business after a disaster and provide necessary evidence in legal matters. For public bodies, the failure to document undermines the principles of accountability and transparency in access to information legislation. When records do not exist where they should, citizens' right of access is denied.[11]

There may also be statutory or other legal requirements for creating and maintaining records. For example, section 35 of the FOIP Act requires a public body to retain for one year personal information about an individual that has been used to make a decision that directly affects the individual. This is to allow the individual a reasonable opportunity to obtain access to the information. An agreement can be reached to retain the information for a shorter period of time.

Transitory Records

A **transitory record** has only immediate or short term value to the organization. Transitory records are not required for future business, legal or archival purposes.

As previously stated, it is the content and context of a record that will determine whether a record is transitory or official. Transitory records typically include personal and social messages, room booking and meeting reminders, direct mail advertisements, outdated blank forms, junk email, copies of documents for reference purposes only, and exact duplicates of records already retained in the organization's records management system (if there are notes on the copy, it is no longer an exact duplicate).

Once transitory records have served their purpose and are no longer of value to the organization, it is important that the emails be disposed of in an appropriate manner. The greater number of emails that must be managed, the harder it is to locate and retrieve information for corporate, access to information and litigation purposes. It also increases costs and manageability for storage and back-up systems. Organizations should consider creating a Transitory Records Schedule that governs the disposition of transitory records.[12]

---

[11] In February 2016, the Information Commissioners of Canada issued a joint statement calling on governments at all levels to create a legislated duty for public bodies to document their deliberations, actions and decisions. The "Statement of the Information and Privacy Commissioners of Canada on the Duty to Document" is available at www.oic-ci.gc.ca/eng/resolution-obligation-de-documenter_resolution-duty-to-document.aspx.

[12] For the Government of Alberta, see Transitory Records Schedule (1995/007-A001) which delegates authority to destroy or delete transitory records to every Government of Alberta employee. Retrieved from www.alberta.ca/managing-government-information.aspx#toc-10.

It is important to note that when an access to information request is received or documents are required to be preserved for litigation, transitory records that have not yet been disposed of must be kept until they are no longer required for such matters.

Also, it is an **offence** to wilfully alter, falsify, conceal or destroy any record subject to Alberta's access and privacy statutes, or direct another person to do so, with the intent to evade a request for access to the record (FOIP Act, sections 92(1)(e) and (g); HIA, section 107(1); PIPA, section 59(1)(c)).

How to Decide Which Emails to Keep

All information that is created, sent or received in the course of carrying out your job responsibilities is a record and potentially an official record. You should keep a record when you need to show what happened, when it happened and who was involved, what was decided or recommended and by whom, what advice or instruction was given, and the order of events or decisions.[13]

To help decide whether an email should be captured as an official record, ask the following questions. If the answer to any of these questions is yes, then the message should be saved as an official record into your organization's records management system:

- Does the message approve or authorize actions?
- Is it a formal communication between staff relating to work?
- Does it signify a policy change or development?
- Does it commit the organization to an arrangement or to a business deal?
- Does it contain advice, provide guidance or constitute formal communications with people inside or outside the organization?
- Am I required to act upon it?
- Is it external correspondence I have received relating to work?
- Is it something that I have sent for a business purpose?
- Is it something I have used at work to make a decision?
- If I left this job tomorrow, would my successor need the information in this message to continue with this matter?
- Is the matter to which the message relates one which may be reviewed or audited later?[14]

---

[13] National Archives of Australia. *Keep the Knowledge - Make a Record.* eLearning Module. Retrieved from www.naa.gov.au/Images/KTK-elearning-text_tcm16-96071.pdf.

[14] State Archives and Records Authority of New South Wales (2017). *Managing email: Email messages are State records.* Retrieved from www.records.nsw.gov.au/recordkeeping/advice/managing-email.

Examples: Should these emails be retained as an official record?

- An email received from a co-worker asking if you want to go for lunch.
    - No, the email is personal and transitory.
- An email received from a co-worker that contains a personal message about a recent vacation and includes as an attachment an update of a project you both are working on.[15]
    - Yes, the email as well as the attachment must be retained as the email identifies the sender and the date and time sent. (Refrain from including personal messages in business emails as the personal message will be become part of the official record.)
- An email from the building management company sent to staff about upcoming building maintenance.
    - It depends. The office manager may keep the email as evidence of action taken on a maintenance issue raised by the office. For other employees, it is likely a transitory record that can be deleted when its purpose has been fulfilled.
- An email sent by you to your manager seeking approval to proceed with a project, and her reply that gives authorization
    - Yes, the email thread is evidence of a decision made.
- An email received from a client asking for information about the status of their application for a program offered by the organization.
    - Yes, the email relates to a business activity.
- A direct marketing email promoting an upcoming conference.
    - No, the email is transitory and can be deleted. An employee or organization may wish to keep the email for reference purposes but it would not be retained in the corporate records management system.

Reminder: Consult with your organization's records management personnel and/or policies and practices if you are uncertain whether an email should be kept.

[15] State Archives and Records Authority of New South Wales (2018). *Training Resource Centre: Email Management – Part A*. eLearning Module. Available from www.records.nsw.gov.au/recordkeeping/recordkeeping-online-modules.

Who Should Capture Official Email Messages?

Ultimately, each employee is responsible for managing the content of their email mailboxes. However, an organization should establish some rules on who should capture emails that are official records to reduce the same email message being saved multiple times into the organization's records management system. These rules may be as simple as:

- If you sent it, capture it;
- If you were the only one who received it from someone outside the organization, capture it;
- If many of you received it from someone outside the organization, the main recipient or the person with prime responsibility for the business documented in the email (e.g. the project lead) captures the message; and
- If in doubt, check with other recipients about who is capturing the message.[16]

Retaining Emails

Emails that qualify as official records may be retained in one of two ways:

- In electronic format and filed in an appropriate electronic recordkeeping system, or
- Printed and filed in the paper file system managed by the organization's records management personnel.

Whether retaining the email in paper or electronic format, the recordkeeping system needs to be able to identify, retrieve, share and retain the records for as long as the emails are needed.

The emails must be saved or retained in a way that ensures they are captured with their transmission and receipt data, and are not changed, thereby remaining accurate and reliable as evidence.

Attachments to emails should be captured and stored with the email message as the message often provides the context for the attachment. If the attachment is going to be worked on, a separate copy of the attachment should be saved for this purpose – the copy becomes a new and distinct record.[17]

As well, emails (and their attachments) should be saved with or otherwise associated with all related records that make up the complete file for that business transaction or activity.

---

[16] Ibid.

[17] Cloy, David. (2007). *Managing Email – Good Practice Guidance* (3rd version). Records Management Office. University of Stirling, Scotland. Retrieved from www.rec-man.stir.ac.uk/documents/ManagingEmail-GoodPracticeGuidancev3.pdf.

Retaining Emails in Electronic Format

To retain emails electronically, an organization might use electronic information management software that is designed to assist with the creation, management, use, storage and disposal of information and records.

There are many different variations of electronic information management software available – below are a few examples:

- Electronic Document Records Management System (EDRMS)
- Enterprise Content Management System (ECM)
- Document Management System (DMS)
- Electronic Document Management System (EDM)

Depending on the functionality of the electronic information management software, emails may be automatically transferred into a file or folder, or "dragged and dropped" into an appropriate file or folder. The retention and disposition of records may be set automatically in accordance with the organization's records retention and disposition schedule, or the schedule may need to be applied manually to the records.

If electronic information management software is not being used, your organization should create or designate an official electronic records repository. The repository should permit formal controls to be set to minimize risk of alteration or deletion and to restrict access to authorized individuals. Emails should be saved with or linked to other official records associated with the transaction or activity – consult with your records management and information technology (IT) personnel to determine the appropriate format in which email messages should be saved to ensure they remain stable and are difficult to alter (e.g. .pdf vs. .msg format). Records retention and disposition will have to be applied in accordance with the records retention and disposition schedule.

Any electronic recordkeeping system should be automatically backed up to prevent inadvertent loss of information.

Other Tips

- You do not need to keep more than one format of your email record. If you have filed your email record in an electronic recordkeeping system, you can delete the copy in your email system (e.g., Outlook). If you have printed and filed your email record in hard copy, you can delete the copy in your email system.
- Emails that are official records should be saved to the designated recordkeeping system (electronic or paper) as soon as possible after they are received or sent, to minimize the risk of being lost or inadvertently deleted.

- Do not save and store emails on your computer hard drive or personal network drive. Doing so limits accessibility to the records and creates a major problem when an employee leaves the organization or a computer hard drive malfunction occurs.

- The loss of transmission and receipt data (metadata) is a concern for the evidential value of printed copies of email messages. If not sure, consult your IT personnel to assure that all metadata are printed with the messages.

- Keep subject lines short and clear using consistent naming conventions when possible. This will help you and the recipient find information and quickly identify relevant emails.

Archiving Emails is Not Effective Records Management

Email archiving is the act of preserving all email to and from an employee. The emails are typically moved from the primary email system/server (e.g. Outlook/Exchange) and stored on another server or storage device. This is sometimes done to preserve the emails of an employee leaving the organization where appropriate email management practices have not been exercised during the employee's tenure. The intent is that at a future date a supervisor will sort through and save the business related emails. Organizations may also archive emails to ease storage issues on the server.

Email archiving is **not** a substitute for an effective recordkeeping system because:

- It does not differentiate between emails that qualify as official records and transitory records such as duplicate, personal and unsolicited commercial email.

- The emails are not linked to related records in other formats and systems.

- Access to the emails is typically restricted to the system administrator or mailbox holder, thus limiting the organization's use of the information captured in the emails.

- Subject lines in the emails may not accurately reflect the content, making it more difficult to search for and find information.

- It is difficult to separate information that is subject to different retention periods, which may result in most information being kept longer than necessary.[18]

[18] Adapted from: State Archives and Records Authority of New South Wales (2018). *Training Resource Centre: Email Management – Part A*. eLearning Module. Available from www.records.nsw.gov.au/recordkeeping/recordkeeping-online-modules.

Staff Training

Effective email management requires ongoing training and support for staff.

As part of their training, staff should be informed of the organization's corporate email management policy and be able to identify what emails to keep as official records and what emails can be deleted; where official email records are to be stored; and that emails subject to an access to information request or litigation hold must not be disposed of.

Most importantly, staff must be aware of how and where official record emails are to be captured and retained (e.g. electronically with information management software, manually moved to a designated electronic repository, or printed and placed on the official paper file retained in the organization's records room).

Training sessions should be required for staff upon their hiring, followed by regular, mandatory refresher training. Staff attendance should be tracked. Organizations should also consider implementing some method for evaluating staff's understanding of the corporate email management policy.

Exit Protocols

When an employee is retiring or otherwise leaving the organization, the employee should ensure that all official email records are transferred from their email mailboxes to the appropriate records management system before they leave. This step should be included in the organization's checklist for exiting employees.

Compliance Assessment

Staff training must be followed with regular monitoring to ensure that records and email management policies and procedures are being complied with and official record emails are being captured in the records management system. One way to assess compliance is to select and review key operational and administrative files where it would be expected that emails would exist.