PROVINCIAL ARCHIVES OF SASKATCHEWAN

Information Management Unit

Effective Date: 2016
Updated: 2016

Email Management Guidelines

Email has become the primary form of communication for most employees of the Government of Saskatchewan. While a portion of email communication consists of information of transitory (short term) value, a significant amount of business critical information that would in the past have been recorded in letters, memos, etc. and filed in an institution's paper record keeping system is now found in employees' emails. Emails created and received as part of government business are considered government (public) records and must be managed in accordance with *The Archives and Public Records Management Act*, which states that records must be retained in a useable and accessible manner until their approved disposal. Examples of emails that are government records include, but are not limited to those that:

- give direction or approval for an action
- record a decision
- give evidence of program or service delivery
- document resource expenditure
- relate to a project you are working on

Not all of the email messages you send and receive will meet the definition of a government record that needs to be classified and retained.

- Non-work related emails are those that do not pertain to government business; they are sent to you as an individual, rather than as a government employee. Some examples include invitations to office social events or emails sent to or received from family, friends or professional associations to which an individual belongs.

- Transitory records do relate to government business, but are of short term use and have no future value. Examples include messages, memoranda or bulletins distributed to all staff, such as staffing updates, notices of building maintenance, HR policies, etc. and emails on which an individual is cc'd for their information but is not required to take any action. For a full explanation of transitory records, please refer to the Archives' Transitory Records Guidelines.

Government institutions must ensure that employees understand their records management responsibilities in regard to email and, as part of their records management program, develop the policy and procedures necessary to manage them appropriately.

Authenticity and Integrity of Email

Emails that meet the definition of a government record must be managed in a way that ensures their documentary and evidentiary value is preserved. From a legal perspective, authenticity and integrity are the characteristics used to determine whether or not records are trustworthy. Email may be required as evidence in court or in other legal proceedings and it is important that the institution is able to demonstrate these characteristics.

> **Authenticity** – an authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have sent it, and to have been created or sent at the time purported.
>
> **Integrity** – the integrity of a record refers to it being complete and unaltered. *The Evidence Act* states that where the best evidence rule applies to electronic records it is satisfied by proof of the integrity of the system that recorded and/or stored the record. Therefore, it is necessary to demonstrate that the system operates properly and that measures are in place to prevent accidental or deliberate alteration to documents recorded by and/or stored in it

In order to demonstrate the authenticity and integrity of email messages, government institutions should establish policies and procedures to ensure that:

- all information identifying the creator, receiver, date and transmission of the message (its metadata) is maintained
- the email cannot be altered and if it is forwarded, the original message must retain its structure, content and context
- an audit trail is recorded
- controls such as access monitoring, user verifications and security are implemented to prevent unauthorized access, alteration, destruction or removal
- measures are in place to prove that the system operates properly and that any system malfunction, upgrade or maintenance does not alter records

Methods of Managing Email

As is the case for all other government records, email must be classified, retained and disposed of in accordance with an applicable approved retention schedule. Ideally, emails should be classified and retained alongside other records that pertain to the activity or business transaction.

Electronic Document and Records Management Software

As is the case with other electronic records, the most effective way to manage email is through the use of Electronic Document and Records Management Software (EDRMS). Features of EDRMS vary depending on the software that is chosen and the ability to manage email may not be included in the base package. However, when this function is added EDRMS will allow institutions to integrate email into its recordkeeping system. Emails are captured in a central repository where they are classified alongside related electronic records, allowing them to be easily searched for, retrieved and disposed of once the applicable retention period is met. EDRMS also incorporate built in authentication, access controls, security, audit logs etc. in order to prove the authenticity and integrity of the records managed by the system. For further information regarding EDRMS, please consult the Information Management Unit.

Until an EDRMS is implemented, government institutions must establish another method of managing email. This can be done using one or a combination of the following:

Print and File

Although it is not the most effective method for their management an institution may direct employees to print and file emails, including their metadata and any related attachments, into its existing hard copy filing system. Once the email is printed and filed, the electronic copy is considered a transitory record and may be deleted from the system. This method integrates the information contained in individual email accounts into a central location where it can be accessed all those who may require it. However, once printed and deleted from the email system the ability to easily and conveniently search for, retrieve and re-transmit documents electronically is lost. Additionally, the print and file approach may not be feasible for all attachments.

If this method is used for the management of email, the institution will still need to demonstrate that the email system operates properly and that measures are in place in order to prove the authenticity and integrity of the records.

Shared Electronic Directories

An institution may instruct employees to capture emails, including their metadata and attachments, into shared electronic directories that mirror the institution's approved classification schedule. Here again, once the email is captured into the shared directory the copy found in the email system is considered a transitory record and may be deleted. This approach allows the institution to integrate emails with related electronic records while retaining the ability to easily search for, retrieve and re-transmit the information. It also allows a complete record of the transaction to be found in one location.

Institutions that use this approach for managing email should give careful consideration to the format in which emails are captured when moved to the electronic directories, as some formats do not capture metadata or attachments. This results in an email record that is incomplete and/or unusable. Institutions must select a format that captures metadata and ensures attachments remain readable, thereby guaranteeing the capture of the complete email, and direct employees to use this format when moving emails to directories. Once transferred to the directories, these records are managed in the same way as other electronic records in a manner that ensures their integrity and authenticity.

Email Security

To a significant extent, the ability to demonstrate the authenticity and integrity of email will depend on the security measures taken to protect the information transmitted by the email system. Government institutions should work with their IT department/provider to ensure measures are in place to protect records from alteration, loss and unauthorized destruction. Examples of such measures include:

- Password Protection – passwords, passphrases or other access controls should be used to protect email systems from unauthorized users. Institutions should set standards and attributes for passwords or passphrases. Employees should keep these secret and change them regularly.

- Message Protection and Authentication Controls – these measures prevent users and administrators from altering an email message once it has been sent to at least one recipient. Users must send a new message with new transmission and receipt data if they wish to change the content of a message. Message protection and authentication controls support the reliability, authenticity, integrity, and version control of email messages.

- System Logs and Audit Trails – system logs can be used to create an audit trail, a record of all actions taken that can be used to reconstruct activity on a given electronic file. Audit trails can be used to either substantiate or invalidate the authenticity or integrity of an email file and the reliability of the email system as a whole.

- Digital Signatures – a digital signature is a small block of data attached to documents being signed. It is generated from an individual's digital ID, as unique identifier that can be obtained from various certificate authorities and registered with programs that support digital signatures. A digital ID includes both a private and public key; the private key is used to apply the signature to the document, while the public key is sent with the file. Government institutions should instruct their employees on the circumstances in which digital signatures ought to be used.

- Encryption – encryption substitutes the text of a message or attachment with a code that only its intended recipient can decode in order to reconstruct the original text. Institutions should advise their employees of the situations in which email messages ought to be encrypted and the encryption methods available to them. Keep in mind that encrypted emails may become inaccessible over time as the method of encryption becomes obsolete. Therefore, these emails should be de-encrypted before they are captured as records, whether this be in EDRMS, on shared electronic directories or in public email folders.

Sensitive, Personal or Protected Information and Email

Government institutions should avoid the use of email for communicating sensitive, personal or protected information unless there is a specific business requirement to do so. Each institution's email policy should outline the main types of sensitive, personal or protected information it holds and identify any information that employees are prohibited from sending via email. In cases where it is permissible to send sensitive, personal or protected information via email, the institution must provide clear

instructions on how this information ought to be sent (for example, personal identifiers must be removed, the message must be encrypted, etc.).

The Freedom of Information and Protection of Privacy Act and Email

Messages in the email system are in the custody or under the control of the government institution and are, therefore, subject to *The Freedom of Information and Protection of Privacy Act*. As with other records, if a FOI request is received no email message that may be responsive to the request, including those considered transitory records, can be destroyed until the request has been completed and all applicable review periods have expired. Emails declared official records that have already been destroyed according to the terms of an applicable approved retention schedule do not need to be recovered. However, if copies of destroyed messages remain in the mailboxes of employees, these will be subject to the FOI request.

Email Management Best Practices

Regularly Delete Transitory and Non-Work Related Email Messages

As previously explained, transitory and non-work related records do not need to be classified and retained. For further information on transitory records, please refer to the Archives' Transitory Records Guidelines.

Use Distribution Lists and the Reply-All Feature Sparingly

Before making use of distribution lists or the reply-all feature, consider whether or not the email needs to be so widely distributed. Use of these features can add unnecessary clutter to mailboxes of individuals who have no need of the information, as well as cluttering the email system as a whole. It also increases the number of emails recipients must sort through in order to decide which messages must be classified and retained.

Identify Who is Responsible For a Message

Because it is common for multiple copies of an email message to exist, it is helpful to set some guidelines that establish who is responsible for managing messages in different circumstances.

● **Sender** - Typically, when email messages are exchanged within an institution, the person who initiated the correspondence is responsible for classifying and filing it. For example, if someone sends an email with a draft of a new policy to five people asking them to review and respond with feedback, that individual is responsible for classifying and retaining the initial email and all subsequent messages related to it. The other five people can delete their copies of the emails.

● **Recipient** – In some circumstances, the recipient of the email will be required to classify and file it. When an individual receives an email from outside of their institution, the recipient is responsible for its classification, as no other copy exists within the institution. If an email received from within the institution gives the recipient directions or authorization for an action, the recipient may wish to retain the email as a precautionary measure so that if that individual is questioned they can account for their actions.

● **Group** - In cases where a group of people work together on a project, committee, task force, etc., it is advisable to assign the responsibility for managing all email messages of the group to one individual. Although the rest of the group may need to keep their copies of the messages for the duration of the project, once it is complete their copies are considered transitory records and can be deleted, since they are assured that the official copy of the messages have been classified and retained by the assigned individual. Alternately, the group may decide to set up a shared folder into which all members may file emails related to the project, committee, etc.

Ensure that Public and Shared Mailboxes are Managed

Public mailboxes are set up for use by a group with a shared need; for example, those working together on a project, committee, etc. Shared mailboxes are designed to provide a point of contact for a particular service, such as help desks or inquiry responses. Responsibility for managing public and shared mailboxes should be assigned to an individual or position. Access controls should be implemented so that only this individual may remove or delete messages from the mailbox. Managing email messages sent to public and shared mailboxes will be easier if the mailbox is used for a single purpose. If this is the case, it is likely that most or all of the messages will be related to the same classification number, so that the individual responsible for managing the mailbox will have few classification decisions to make.

Limit the Content of Email Messages to One Topic

Email messages that discuss several topics may be difficult to file, as more than one classification number may apply to them. Limiting email messages to one topic will make it easier to determine how a message should be classified.

Roles and Responsibilities

Individuals at all levels of the institution have a role to play if email is to be properly managed.

Institution Heads and Executive Management

● set the strategic direction for email management and provide sufficient resources and support for email management programs and systems

Program Managers

● identify training needs of employees in regard to email management and ensure training is provided
● monitor employee compliance with email management policy and procedures

Records Management Coordinator

● develop, implement and ensure consistent application of the institution's email management tools, standards, policies and procedures
● provide education and advice on e-mail management to employees

IT Staff

- assist the institution's Records Management Coordinator in the development and implementation of email management tools, standards, policies and procedures
- create, maintain and preserve system documentation in order to provide proof of the authenticity and integrity of the institution's email messages

All Staff

- understand and comply with the institution's email management policy and procedures
- manage email that meets the definition of a government record in accordance with an approved retention schedule as per *The Archives and Public Records Management Act*
- delete personal email and transitory records from the email system regularly
- take appropriate precautions when sending email messages that contain personal or confidential information