Kansas Email Guidelines Task Force
Proposed Updates to ITEC Guideline 6401 -- Managing Electronic Mail
Version 2
ITEC Approved Effective 6/9/2020

1 Scope

All state and local government entities in the State of Kansas are encouraged to use these guidelines.

2 Purpose and Intent

The State Records Board and the Information Technology Executive Council present these guidelines as an overview of current principles and best practices for managing electronic mail (email) records. Their purpose is to ensure that Kansas state and local government email records are retained for as long as they have legal, fiscal, administrative, or historical value. The guidelines are intended to complement existing retention schedules and to serve as a common starting point for state agencies and local governments in formulating their own email records management policies and procedures. Kansas state and local government entities should adapt the guidelines to meet their specific needs and capabilities.

3 Definitions

3.1 Government records

The Government Records Preservation Act (K.S.A. 45-402(d)) defines government records as "all volumes, documents, reports, maps, drawings, charts, indexes, plans, memoranda, sound recordings, microfilms, photographic records and other data, information or documentary material, **regardless of physical form or characteristics**, storage media or condition of use, made or received by an agency in pursuance of law or in connection with the transaction of official business or bearing upon the official activities and functions of any governmental agency."

3.2 Email

Email is an asynchronous message sent via a computer network that includes a header, body, and, optionally, attachments.

3.3 Email records

Email sent or received in the conduct of government business is considered a government record and is subject to records retention requirements and open records requests. Email is not a type of record with a single retention period. Email is a method of communication and the retention period for an email depends upon the content of the message.

3.4 Non-record email

Non-record email includes listserv messages, advertisements, news articles, personal messages, and spam. Non-record emails may be destroyed immediately.

3.5 Capstone approach

The Capstone approach to email management bases records retention requirements on the account owner's role or position rather than individual email content. Email accounts are designated as either permanent or temporary, based on the reasoning that email with permanent value in documenting the agency's core functions is most likely to be produced by certain account holders such as senior officials and other key decisionmakers, while much of the rest is either duplicate or temporary. The National Archives and Records Administration developed the Capstone approach in 2013 as a means of simplifying and automating email management.

4 Capstone Email Management

4.1 Identifying a Capstone account

Capstone is an approach to managing email, it is not a type of technology. When adopting the Capstone approach, agencies should identify those email accounts most likely to contain records that should be preserved as permanent. Agencies will determine Capstone accounts based on their business needs. They should identify the accounts of individuals who, by virtue of their work, office, or position, are likely to create or receive permanently valuable government records. Capstone officials will generally be the top-level senior officials of an agency but may also be other key decision makers at lower levels of the agency. The *Kansas Capstone Accounts Identification Worksheet* will help agencies identify relevant accounts.

4.2 Agency responsibilities for maintaining email

Capstone can reduce the burden on individual end-users by encouraging the greater use of automated methods for managing email accounts. Agencies are responsible for managing Capstone email records in accordance with retention and disposition schedules. When using the Capstone approach for capturing and managing email, agencies must continue to:

4.2.1 Ensure email records are scheduled

Agencies should work with the State Archives to ensure email records are covered by a retention schedule. This may include creating new schedules, using existing schedules, or using an applicable General Records Schedule.

4.2.2 **Ensure proper retention and disposition of records**

In addition to developing retention schedules, agencies should ensure the proper maintenance of active records. Once the retention period has been met, agencies should ensure the proper transfer or storage of permanent email records and destruction/deletion of non-permanent email records.

4.2.3 **Prevent the unauthorized access, modification, or deletion of declared records**

Agencies must ensure the email repository has appropriate security measures in place to prevent unauthorized access to and/or destruction of records. Records must retain authenticity, reliability, and trustworthiness throughout capture, maintenance, and transfer.

4.2.4 **Ensure all records in the repository are retrievable and usable**

Email records maintained in a repository must be accessible to appropriate staff for as long as needed to conduct agency business. Agencies should also consider retrievability and usability when migrating from one repository to another.

4.2.5 **Consider whether email records and attachments can or should be associated with related records under agency guidance**

As a supplement to the Capstone approach, an agency may need to connect email records, such as those associated with case files or project files, with other related records. This may be accomplished by:

- Using electronic pointers (such as metadata tags) to establish linkages, or
- In select cases, filing with associated paper or electronic case or project files.

4.2.6 **Capture and maintain required metadata**

An agency should ensure that email metadata are preserved. Standard metadata elements include the date of the email and the names and email addresses of all senders and recipients particularly if the system uses nicknames, distribution lists, or a blind copy feature. The agency may wish to retain and preserve additional metadata for legal and business purposes. Regardless of the repository, agencies should examine email upon transfer to another repository or to the State Archives to ensure that names and addresses are appropriately associated with each email. Agencies should also work with vendors and their information technology departments to confirm that their repository is capturing and can export the necessary metadata elements.

4.3 Managing a Capstone email account

Following Capstone, an agency should schedule all the email in Capstone accounts as permanent records.

At the end of an employee's tenure in a Capstone position, Capstone email accounts should be preserved permanently by the agency or transferred to an archives following resolution of any litigation or legal hold issues.

4.4 Managing a non-Capstone email account

Non-Capstone users are responsible for managing their email according to retention and disposition schedules.

5 Email Classifications

5.1 Correspondence – Policy Related (Permanent)

These records are defined as:

> Incoming and outgoing letters, memoranda, and email records that state or form the basis for policy, set precedent, or record important events in the operational and organizational history of the agency. These may include Capstone or non-Capstone account correspondence.

Agencies must retain records in office until the employee leaves the position, then records are kept permanently or transferred to an archives.

5.2 Correspondence – Routine

These records are defined as:

> Incoming and outgoing letters, memoranda, and email records that pertain only to routine matters and are not identified in another record series.

Agencies should retain records until the business is completed, then destroy.

5.3 Correspondence – Retention schedule specific – retained in accordance with retention schedule

These records are defined as:

> Incoming and outgoing letters, memoranda, and email records that pertain to a specific government function.

Agencies should retain these records according to the associated general or agency schedule entry. (EX: Retain correspondence related to budget preparation files according to series 0016-000.)

6 Best Practices

6.1 Agency email policy

Business functions of individual agencies vary, so a one-size-fits-all email policy is nearly impossible to create. The information in this document is intended as a guideline for email management. Agencies should develop their own agency-specific email policies using these guidelines that address key issues. These issues include:

- Email ownership – email is a government record and is subject to the Kansas Open Records Act.
- Appropriate use of email – agencies should indicate what is considered appropriate use
- Email security – the policy should address passwords, phishing, ransomware, and other security issues the agency deems important.
- Records management expectations – agency policy should address the end-user's role in managing their email for proper records management techniques.
- Transmission of confidential and sensitive information - agency policy should address proper transmittal of sensitive or confidential information through email.

6.2 Email threads

An email thread is a group of related email records consisting of replies to or forwards of an original email. Since email threads often contain important contextual information about agency activities, the full thread should be maintained in accordance with the applicable retention requirements. It is best practice to avoid deleting individual messages from an email thread and to refrain from changing the subject line in the middle of a thread.

6.3 Attachments

Attachments are electronic files associated, transmitted, and stored with an email record. Attachments may include essentially any file format including text, graphics, spreadsheets, video, and audio files. Agencies should ensure that attachments maintain their association with the original email record throughout the required retention period. If an email is transferred from the email system to an external electronic recordkeeping system, any attachments should be moved and remain associated with the original email record.

6.4 Filing system (folders)

Each user should organize email to aid in the filing and retrieval of messages. This should be done through a system of folders and subfolders. After a brief period in the user's inbox, messages should be transferred to properly titled folders or subfolders related to a specific work function, project, or program. Tags or labels may also be used.

6.5 Managing email outside of the email system

Agencies should manage records within the email system as much as possible. Printing or saving email records as PDFs is not encouraged, as that requires more work for the end-user. Utilizing proper filing systems with tags and labels will ensure proper records management of records within the email system. If an agency has a document management system, email records may be stored in that system.

6.6 What happens to an email account when an employee leaves a Capstone position and/or leaves the agency?

6.6.1 Capstone Accounts

When an employee leaves a Capstone position the agency should collaborate with the Office of Information Technology Services (OITS) or their IT staff to:

- place the account on litigation hold;
- generate a data file for the account;
- transfer the data file to the State Archives or retain permanently.

6.6.2 Non-Capstone Accounts

When an employee leaves a non-Capstone position the agency should collaborate with OITS or their IT staff to:

- generate a data file for the account;
- transfer the data file to the agency, which is responsible for retaining the email records in accordance with retention requirements.

6.6.3 Other Considerations

- Email records in active use by an agency will likely need to remain accessible to the agency. If possible, the original record source (i.e. user mailbox) should be kept in an immutable (read-only) state. Depending on the environment and agency needs, records may need to be copied to another location (another user's mailbox, file share, collaboration system, etc.) to maintain accessibility, but this may result in the creation of a "new" record that will also be subject to retention policies.
- It is advisable for agencies to take steps to prevent accidental or malicious destruction of records when an email user leaves employment. These steps should include putting into practice policies and procedures appropriate for the agency's environment as well as providing users adequate training. For example, it may be wise to caution users against simply deleting all of their stored email as "housecleaning" before leaving the agency, but to instead make an effort to avoid unintentionally destroying records that need to be retained.

- Records intended for long-term retention would ideally be kept in a format that can be accessed even without the originating system, but this may not be possible or practical for all agencies. Therefore, it is recommended that agencies at least consider format compatibility for new and existing records when planning changes to their email and archival environments.

6.7 KORA and Public Records

6.7.1 Purpose

The Kansas Open Records Act (KORA), K.S.A. 45-215 et seq., governs access to public records. Under the KORA, public records are open for inspection and copying by any person unless otherwise provided by law.

6.7.2 Application

The KORA applies to any public records, regardless of form, characteristics or location. This includes emails.

A public agency must search for all records that are covered by a KORA request, including emails. When searching email, the public agency should establish and document the search terms used to locate responsive records.

6.7.3 Limitations

The KORA only requires a public agency to provide access to or copies of records it has at the time the request is made. It does not require a public agency do research, create a record, or answer questions.

6.7.4 Discretionary exemptions

The KORA contains some 55 categories of records that public agencies may, but are not required to disclose. There are many other Kansas laws that mandatorily close certain records.

Agencies are strongly encouraged to consult with legal counsel regarding the KORA's requirements.

6.8 E-discovery

6.8.1 What is e-discovery?

E-discovery is a pretrial legal process used to obtain and review electronically stored information (ESI). ESI can include any data or data compilations. This includes email records.

6.8.2 Rules governing e-discovery

The rules governing discovery of, and the process used to obtain, ESI vary by jurisdiction (e.g., federal or state). They also vary by the nature, size and type of case (e.g., civil, criminal or class action).

6.8.3 **Consequences for improper handling of ESI.**

The consequences for improper handling of ESI in the context of litigation can be dire, up to and including adverse inference instructions following loss or destruction of ESI. In its most severe form, a court may instruct a jury that certain facts are deemed admitted and must be accepted as true. Such an instruction can be an outcome-determinative sanction.

6.8.4 **Best practices**

At a minimum, an agency must work with its legal counsel and IT staff to establish information and data governance processes. Such processes should:

- recognize and plan for the possibility of litigation and discovery, including e-discovery;
- ensure that relevant records are, and remain, available and usable for the duration of any litigation and any appeals;
- protect and secure the integrity of any ESI or other data;
- give consideration to ESI in legacy data and email systems; and
- ensure the preservation of the records for later use if necessary.

This guidance is not intended to be a substitute for informed legal advice. Agencies are strongly encouraged to consult with legal counsel concerning e-discovery.

6.9 **Litigation or Legal Holds**

6.9.1 **What is a legal hold?**

A litigation or legal hold is a process for preserving paper and electronic records, and other related information, when litigation is reasonably anticipated. This includes email records.

A legal hold suspends normal destruction practices to guard against spoliation of evidence. Spoliation can involve the destruction or alteration of evidence. Spoliation of evidence carries a substantial risk of sanctions for failure to preserve ESI or other information/records.

6.9.2 **Identify events that may trigger a legal hold.**

An agency should designate its general counsel or other member(s) of its legal department to be responsible for identifying events that may indicate the potential for litigation and the corresponding need to suspend destruction of records.

6.9.3 **Communication about the legal hold.**

The agency's general counsel or designee should establish a process for communication about, and periodic review of, legal holds. Legal holds may be reissued or amended as necessary, depending on the circumstances.

6.9.4 **Some things to consider if a legal hold is necessary.**

If a legal hold is warranted, the general counsel or designee(s) should work with IT staff and others as necessary to:

- communicate written notice of the legal hold to affected individuals;
- obtain a written acknowledgment of the legal hold from affected individuals;
- identify, collect and preserve all potentially relevant information/records, including ESI;
- sequester or segregate information/records from normal retention processes to prevent destruction or deletion of records either inadvertently or deliberately; and
- take steps, including compliance audits, to ensure legal hold information/records are not destroyed until resolution of any litigation, including any appeals

6.9.5 **Things to consider once a legal hold is no longer necessary.**

Once the need for a legal hold has been resolved, the agency's general counsel or designee should:

- release the legal hold;
- allow normal retention and disposition processes to resume; and
- provide written confirmation to the affected individuals that the legal hold has been released and normal record disposition processes may resume.

This guidance is not intended to be a substitute for informed legal advice. Agencies are strongly encouraged to consult with legal counsel regarding legal holds.