Email Management

Summary
An electronic mail message or “email” consists of a digitally created, transmitted, and stored message and any attached digital documents. State and local governments use email for a variety of tasks such as sending and receiving internal and external correspondence, distributing memos, circulating drafts, disseminating directives, transferring official documents, and supporting various business processes of the organization. As such, email messages are potentially official government records, and as both state statutes and case laws make clear, email must be included in your overall records management strategy.

Email documents that hold information about the day-to-day operations of state and local government must be easy to locate; those that hold information of long-term or permanent value must be adequately protected; and those with transitory value must be deleted when no longer needed. Allowing email to be managed by personal preference or routine system back-ups and administrative procedures that treat all email alike can result in serious legal, operational, and public relations risk. By establishing policies, applying records management procedures, and training users, you can create an environment that promotes successful management of email records.

Legal Framework
For more information on the legal framework you must consider when developing an email records management policy refer to the Legal Framework chapter of these guidelines and the Minnesota State Archives’ Preserving and Disposing of Government Records. Also review the requirements of the:

- Official Records Act [Minnesota Statutes, Chapter 15.17] which:
  - Mandates that government agencies must keep records to fulfill the obligations of accountability and stipulates that the medium must enable the records to be permanent.
  - Stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court. This stipulation means that you can copy your email messages to paper or to text files, as long as the record’s content, context, and structure are intact.
  - Does not differentiate among media. The content of the email message determines whether the message is a record.

---

Electronic Records Management Guidelines
Email Management

- **Records Management Act** [Minnesota Statutes, Chapter 138.17[^3]] which establishes the Records Disposition Panel to oversee the orderly disposition of records, including email records, using approved records retention schedules.

- **Minnesota Government Data Practices Act (MGDPA)** [Minnesota Statutes, Chapter 13[^4]] which mandates that government records should be accessible to the public unless categorized as not-public by the state legislature. Managing access to public versus not-public email records is especially important because email is so easily forwarded, misdirected, and sent to groups of people.

- **Uniform Electronic Transactions Act (UETA)** [Minnesota Statutes, Chapter 325L[^5]] and Electronic Signatures in Global and National Commerce (E-Sign)[^6] [a federal law]. Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

### Additional Legal Considerations
Within the context of the above laws, you should also consider:

- **The ramifications of the Armstrong litigation.** One of the first legal cases utilizing e-discovery, was Armstrong v. Executive Office of the President (1 F.3d 1274 [DC Cir 1993]). In this case a federal court found in favor of a group of researchers and nonprofit organizations who wanted to prevent the destruction of email records created during the Reagan administration. The court determined that federal government agency email messages, depending on content, are public records and that complete metadata must be captured and retained with the email record. Although a federal decision, this litigation strongly influenced government agencies at all levels, and agencies began paying closer attention to their email records management practices, including the capture of metadata.

- **The ramifications of Zubulake v. UBS Warburg LLC.** The 2003 case of Zubulake v. UBS Warburg LLC has also been a major influence on the courts when determining what electronic records need to be produced during litigation. The five decisions from this case help provide a baseline standard of what needs to be available for litigation purposes; including ensuring that all relevant documents are able to be discovered, retained, and produced when necessary.[^7] The Zubulake decisions also prompted the idea of a ‘litigation

hold’ on electronic records. This hold ensures that documents, if they relate to current or future litigation, must be retained as long as necessary, including past their retention period if it has already past.

- **Legal discovery.** When developing your electronic records policy, balance your legal and operational requirements with the risk of being engaged in legal discovery. You must meet all government requirements for managing your email records, but you should also be able to respond to discovery in an affordable, efficient, and practical way. In 2006, the Federal Rules of Civil Procedure (FRCP)\(^8\) were amended to specifically address discovery issues for “electronically stored information”, including email.

### Key Concepts

As you develop your email records management policy, you will need to be familiar with the following key concepts:

- What is Electronic Mail?
- Other Electronic Messaging Systems
- Determining Value of Electronic Messages
- Retention and Disposition of Electronic Messages
- Managing Documents and Metadata
- Developing an Email Policy
- Training for Staff Members
- Processes for Preserving Email

### What is Electronic Mail?

Email can be a confusing term because it can refer to both a system and the messages within a system. Furthermore, it can also be used to describe the action of sending or receiving a message. Here are some basic definitions to help clarify the process:

- Email *Systems/Clients:* Email systems or clients are the applications that enable users to compose, transmit, receive and manage text and/or graphic email messages and images across networks and through gateways connecting the latter with the Internet. Applications may be

text or graphics-based, proprietary or open-source, public or private. A common email application is Microsoft Outlook, which many organizations sue as a front-end to Microsoft’s Exchange Server. Some organizations are moving to vendor-hosted solutions such as Gmail for Business, to provide online staff access to email and as a cost-saving measure.

- Email Messages: The communication supported by email systems sent between individuals or groups of individuals. The contents of the communication, the transactional information (metadata) associated with each message, and any attachments to the body of the message are all part of an email message.

- Email Server: The hardware on which the application resides and is used to route and store large volumes of email. Servers can be housed internally in your organization and managed by IT staff or housed and managed by others at a separate facility. If managed by an outside agency, proper security measures must be taken to ensure record authenticity and trustworthiness.

- Transactional information: Transactional information records the information, or metadata, about an email message. This metadata can include the name of the sender and all recipients, the date and time the message was created and sent. It may also include information on the systems and software applications used to create and transmit the message. Transactional information may not always be visible in every application but it is a vital part of every message and steps must be taken to preserve it. The federal courts have ruled that this information is a vital part of the message itself, and is an important consideration when storing email messages.

Other Electronic Messing Systems

In addition to email, there are other electronic messaging systems available to most organizations; they include voicemail, instant messaging, and text messaging. If used for official government purposes, a message created and managed in these systems may also be considered a record.

Therefore, when developing an email management program, organizations should also review all messaging systems in use and include any records covered under the existing records retention and disposition process. Work with your records management staff to develop new schedules where needed. Refer to *Preserving and Disposing of Government Records* for more information on retention schedules.

Voicemail

Voicemail is a computerized system for receiving, recording, saving, and managing voice messages. Although telephone-based voicemail is well-established in many organizations and

---

used for important public business, it has rarely been managed as a record.

Technological advances that blur the distinction between email and voicemail could make it easier to capture and manage audio records. Services utilizing Voice-over-Internet-Protocol (VoIP) are capable of delivering messages as audio files via email. Therefore, voicemail messages saved as email can be managed along with other email relating to the same topic. However, VoIP uses the Internet, and messages sent this way are subject to the same security threats as other Internet communication methods.\(^\text{11}\)

**Instant Messaging**

Instant messaging (IM) is a service that permits individuals to quickly exchange electronic messages with selected others in an informal manner that mimics conversation. Instant messaging differs from ordinary email in the immediacy of the message exchange that makes a continued exchange simpler than sending email back and forth. Most exchanges are text-only, however, some services allow voice messaging and file sharing. There are systems available to help organize, preserve, and provide access to Instant Messages over time. They often treat IMs the same as email communication.

**Text Messaging**

Text messaging, or texting, is another communication tool frequently being used. Text messaging uses mobile technology to send short bits of communication from one location to another. At times, these messages replace email or phone communications. If used for official government business, these types of messages should be considered when addressing your records management policy. Because space is often limited, users have developed a texting shorthand that uses abbreviations and code words for common phrases. If necessary, text messaging should be addressed in a general policy manual including when it can be used, and how to document the messages long-term if necessary.

---


Determining the Value of Electronic Messages

Not all email requires the same level of control. Although identification of email records relating to the activities of public organizations will always be subjective, certain categories of records will typically be important to identify and manage.

These include:

- Policies and directives
- Work schedules and assignments
- Drafts of documents circulated for approval or comment
- Any document that initiates, authorizes, or completes a business transaction
- Final reports or recommendations
- Correspondence, memos, or messages about agency business
- Agendas and minutes of meetings

Transitory and personal messages that do not support government business, as well as convenience or duplicate copies of email records, should be deleted from mailboxes when no longer needed. These include copies or extracts of documents distributed or received for reference — listserv or bulletin board posts, personal messages, announcements unrelated to official business, and announcements of social events like retirement parties or holiday celebrations. These materials consume disk space, erode the efficiency of the system, and, if kept, could be subject to information requests and discoverable in legal proceedings.

Retention and Disposition of Electronic Messages

When thinking about email records and retention schedules, it is important to remember that retention periods are based not on the method by which a record is created but rather on the content, and on the legal, fiscal, administrative, or historical value of the information contained in the record.

You must prepare record retention schedules in accordance with the Records Management Act to retain or dispose of all official copies of email records relating to government business. Generally, records transmitted through email systems will have the same retention periods as similar records in other formats. Email letters and memos, for example, will be retained and disposed of according to the retention periods established for various types of correspondence. Many email messages will be part of a distinct record series. Those messages should be retained and disposed of according to the retention period established for that series.
The Minnesota State Archives has gathered together, on its website\textsuperscript{12}, several general record schedules for many types of records, for state, county, city, and township government records, including correspondence. Records having no significance beyond their initial use and when no longer needed for reference, should be destroyed according to an approved retention schedule. Keep in mind that simply deleting a message may not remove it completely from the storage media. Utility programs and other tools are available to permanently remove electronic messages and eliminate the possibility of recovery. Retention schedules must be approved by the Records Disposition Panel.

### Managing Documents and Metadata

Although your agency will develop unique procedures that meet your specific operational and legal requirements, bear in mind the following goals for an email record. An email record should be:

- **Complete**: Email records should completely document the transaction. For example, you cannot save the text without the sender information. Complete email records must include all of the following elements, as applicable:
  
  - Names of both the Sender and Recipient(s)
  - Date and Time Sent
  - Subject Line: Clearly describing the contents of the message (e.g., the subject line ‘correction’ is inadequate. ‘Correction to Tourism Board Minutes 2005March15’ provides a better description.
  - Body of email
  - Attachments should be included in full (not just indicated by file name).
  - If a distribution list was used to send a message, a list of the names of individuals who are part of the distribution list needs to be recorded. This provides a way to identify the actual recipients if the email record simply lists the group name in the recipient field. For example, the distribution list “HR” (a distribution list for all the individuals of the human resources department) should be documented so that each individual of the list is named.
  - Directory of email addresses and the corresponding staff member names (e.g., jado25@myorg.net is Jane Doe). This connects an email address listed in an email record to a person.

- **Accurate**: The contents of the email record should accurately reflect the transaction.

[http://www.mnhs.org/preserve/records/retentionsched.html](http://www.mnhs.org/preserve/records/retentionsched.html)
Electronic Records Management Guidelines
Email Management

- **Accessible.** Unless otherwise classified under the MGDPA, email records must be accessible to the public. All email records, like other electronic records, should be reasonably accessible for the purposes of legal discovery.

- **Manageable.** Email records should be easy for staff members to manage as part of the daily workflow and records management practices. Because staff members will implement and use the email records management policy, procedures should be straightforward.

- **Secure.** The email record should reside in a secure system that controls access, storage, alteration, and deletion. This is particularly important in controlling access to non-public content. Email records present unique security concerns, because email messages are:
  
  - Easily manipulated or deleted in the system.
  - Easily captured and read by unintended persons.
  - Easily forwarded and misdirected by mistake.

### Developing an Email Policy

You should establish policies to guide users about appropriate email practices. Policies should answer questions about acceptable use, explain the management and retention of official copies, and discuss privacy and access issues of email. When developing a policy, you should make sure to receive input from all stakeholders, allow stakeholders to review and comment on the policy before it is finalized, test the procedures, and train staff. The policy itself should also be documented and all users should understand these policies and be able to apply them. More information about general policy topics is provided below.

**Acceptable use**

Written policies should be established for the use of email (and other electronic communication methods) in the same way they are established for the use of the telephone, fax machine, and postal mail.

**Staff roles and responsibilities**

Your policy should clearly define the roles and responsibilities that managers, network administrators, technical staff, records management staff, support staff, and users will have in the management of email. It should clearly communicate whether the sender or the receiver should save email records. The policy should guide staff members in determining which email messages are records and outline a procedure for grouping emails into records series with a records retention schedule for each series.

**Management and retention**

Because the Records Management Act requires custodians to protect their records and to work with the Records Disposition Panel to establish retention periods, your policy should describe
how and where you will maintain the official copies of your email and provide for their management, protection, and retention for as long as they have administrative, legal, fiscal, or research value.

**Filing and maintenance**

Only the official copy of email records that relate to agency or local government business functions need to be filed and maintained in a recordkeeping system. Additional copies, transitory communications, and personal messages can simply be deleted from the email system when no longer needed. A policy should include procedures for organizing, storing, maintaining, accessing, and disposing of email records. Your policy should define how users are to manage their accounts including the regular removal of personal and transitory messages from their mail boxes.

**Privacy**

Your policy should make it clear that although you attempt to provide security, email messages sent or received are not private. They may be accessed and monitored by others, may be released to the public, and may be subject to discovery proceedings in legal actions. Because computers can store messages at multiple locations within the system, even messages a user has deleted may be recoverable and used in a legal action.

**Access**

Because government email can be defined as a public record, email policies must comply with the state’s MGDPA and Records Management Act. MGDPA gives the public the right to access records, but it also limits access to some information considered personal or private. Custodians of public records must make their records available for public inspection provided that the information is not exempt from disclosure.

**Documentation**

In addition, you should establish a procedure for documenting your email records policy. On an on-going basis, from initial development onward, document the development of your email records management policy, the policy itself, and changes to the policy. Include a description of the software and hardware in use, any training provided to staff, staff member responsibilities, and records retention schedules.

**Training for Staff Members**

All agency employees should be trained in using the records retention schedule to identify and classify the records they create. They should be aware of proper retention and disposition procedures and who to contact when records need to be transferred out of their custody. Because individuals have direct control over the creation and distribution of email messages, agencies should provide training for their employees on agency email procedures. Depending on the type of email and recordkeeping system an agency uses, the policy and procedures will vary.
Agencies will want to be sure that employees can answer legal and operational questions about email. Any training and documentation materials should set forth guidelines that will allow employees to answer questions about the legal and operational value of their records. Possible questions that employees can ask themselves include:

- Is this email an official record? Is this email message business or personal (e.g., “Thursday staff meeting to start an hour late.” or “Let’s do lunch!”)?
- Does this email message have long-term significance (e.g., “New policy finalized.”)? Does this email message document a transaction or operations function (e.g., a process, a decision, or a discussion)?
- Is this email record public or not-public as set forth by the MGDPA?
- What metadata must I capture when I save this email record?
- Which records series does this email record belong in?
- Should I save the complete email record, including attachments and group list names?
- Could this email message ever be required as evidence in a legal action?
- Who is responsible for retaining the official copy of an email?
- This flowchart\(^\text{13}\) is used by the Kentucky Department of Library and Archives to manage email messages. A similar diagram could be developed for your institution.

**Processes for Preserving Email**

Government agencies have responsibility for developing guidelines and procedures to incorporate email messages into their overall recordkeeping. Agency administrators should also develop policies and systems designed to ensure that email records are appropriately preserved, secured, and made accessible throughout their established retention periods. Procedures and systems configuration will vary according to the agency’s needs and particular hardware and software used.

Agency records of long-term value should not be stored on individual workstations. The records should be stored on a secure drive that has the proper security features to protect the records from alteration or destruction and to provide regular back-up. Offsite employees with laptops and other personal devices should download their messages to the agency’s network drives on a regular schedule. Simply backing up the email system onto tapes or other media or purging all messages

\(^{13}\) Kentucky Department for Libraries and Archives. *How Long Should I Keep My Emails* [http://kdda.ky.gov/records/recmgmtguidance/Documents/Email training/E-mail diagram-state.PDF](http://kdda.ky.gov/records/recmgmtguidance/Documents/Email training/E-mail diagram-state.PDF)
after a set amount of time is not an appropriate strategy for managing email.

There are three ways to preserve email messages: online, near-line, and off-line. Each method has its advantages and disadvantages; each requires a different degree of technical support; all require supervision and management. In making your selection, be sure that:

- it meets the needs of users;
- it complies with all recordkeeping requirements;
- you have the tools, written policies and procedures in place; and
- users understand the policies and procedures, are familiar with the tools, and can apply all three consistently to all records.

Brief descriptions of each method are listed below.

**Online Storage**

Online storage can maintain email messages within the email application itself. This is a good method for storing temporary and short-term records (less than 5 year retention). Microsoft Outlook does have limited capability to carry out this approach which can be employed by using the “archiving” function in the application.

Another method of online storage requires the establishment of an electronic filing process using a secure shared network server. The filing process should be used to collect and store related electronic records including, but not limited to, email. Staff should be appointed to oversee the process and system including the establishment of naming protocol and file structure as well as be responsible for assigning access privileges to the system including delegation of privileges to add, delete or edit specific files and records.

Keep in mind that email systems are not recordkeeping systems, and messages should only be stored short-term within an email system. Retaining important email within the email system disconnects it from other related information and makes it susceptible to loss through regular system purges. It will be up to you to determine the amount of risk being taken for storing files within an email application.

**Advantages.** You retain the ability to easily search for, retrieve, or retransmit messages electronically. You may also retain important information related to the distribution of the email. Depending on the filing arrangement used, it may be an effective way to integrate similar records that are created and received in electronic form.

**Disadvantages.** The process requires active participation of all email users. If not consistently and accurately managed, records are difficult to locate. Unless all records are in electronic format, you will also have to coordinate filing systems for records in both paper and electronic formats. It requires the use of a separate secure shared drive controlled by a limited number of employees to protect official copies from unauthorized access and prevent storage of duplicate
Near-line Storage
Near-line storage involves the transfer of the email messages and transactional information into an electronic recordkeeping system other than the email system itself. For example, an email message dealing with a particular project could be stored in a file on the agency’s network drive with other electronic files dealing with the same project. The message still retains some of its functionality, including the ability to be indexed and retrieved electronically. If the agency stores other records in electronic format, then the email messages can be integrated with other related project files.

Disadvantages to storing records near-line are the potential costs for the equipment, maintenance and service for the electronic recordkeeping system. The agency should consider the costs and benefits, and the compatibility of their email application and the electronic recordkeeping system. Storing messages external to the email application may mean converting the messages to a different format, which could result in the loss of important information. Records with retention periods of more than 5 years need to be migrated and possibly converted to new formats and systems as older ones become outdated. Finally, if the agency still maintains many of its records in paper, then the two systems (paper filing system and the electronic system) must be integrated and work together.

Off-line (Paper) Systems
In some cases, especially for permanent and long-term records, the best preservation solution may be to print the email messages, and transactional information, onto paper. This solution makes sense if the agency does not already have an electronic system in place that is designed for long-term records protection and accessibility or if a majority of its records are kept in paper form.

The biggest advantage to off-line storage is the stability of the medium. Agencies do not have to worry about hardware and software becoming outdated and the records becoming irretrievable. Email messages can be filed with other records of the same type or series directly, making the retention and disposition process easier.

The disadvantage is that the email messages lose their dynamic functionality as electronic documents. They cannot be searched and retrieved as quickly and efficiently as in a well-managed electronic system. You may also lose important information related to the distribution of the email. Furthermore, documents can be misfiled when users are responsible for printing, routing, and filing their own. Finally, with the pervasive use of email applications in the course of government business, the volume of paper records will build up quickly.

Note: No matter what storage option the agency chooses, transactional metadata must be properly captured and stored with the email message for the full value of the document to be preserved.
This task is usually easy in email applications that readily display this information. Applications that do not display the metadata need to be configured so that the data stays with the message in whatever form the message is retained.

Keep in mind that access to email is no longer tied to an individual work computer. Email can generally be accessed from anywhere with an Internet connection. Wireless Internet connections and mobile networks make it possible to send and receive messages from almost any location. If official business is taking place in multiple systems, including through personal accounts and devices you must be sure to have methods of capturing all relevant transactions.

**Key Issues to Consider**

Now that you are familiar with the operational and legal importance of managing email messages as records, you can use the questions below to begin the development of your email management policy. Discussion of the questions below will help:

- Ensure that you meet your legal and operational requirements
- Gather staff member input, support, and compliance with your email management policy
- Integrate your records management policy with your overall electronic records management strategy
- Ensure that staff members manage email records at the appropriate points in the records continuum, rather than as a single records series with one retention schedule (as explained in the *Electronic Records Management Strategy* chapter of these guidelines)

**Discussion Questions**

- How can we ensure staff member compliance and understanding? What process is reasonable to ask staff members to comply with?
- How should we train staff members? How accountable should we make staff members for compliance?
- How should we develop our process?
- Which email messages are official records?
- What elements of an email record are required for a complete understanding of the transaction?
- What is the appropriate records series and records retention schedule for each records series? How should email records be organized for long-term storage and access (e.g., project,
department, function)? How will we retrieve and dispose of email on our chosen storage media?

- How should our email retention strategy coordinate with our other records management procedures (e.g., store all project-related email with the other project documentation)? What documentation do we need for our process?

- How should we implement the procedures technically and operationally? How can we plan our implementation so the policy is widely used and accepted, but causes minimal disruption to our daily operation?

- How will this all be documented?
Annotated List of Resources


This report provides practical advice on how to ensure email remains accessible over time and address the technical, legal and cultural challenges of email preservation.

http://www.statearchivists.org/arc/states/res_emai.htm

Resources specifically about electronic mail policies compiled by state.

ARMA International. *Home Page*. 
http://www.arma.org/

“ARMA International is the oldest and largest association for the records and information management profession.” This website provides users with access to publications and information about electronic records management, standards and best practices, professional development, and upcoming conferences and seminars. Local chapters of ARMA have been developed in many metropolitan cities, of which a list can be found on this ARMA International site.

The Sedona Conference. *Publications Home Page*. 
https://thesedonaconference.org//publications

Publications address issues of eDiscovery, Email management, and other topics. (Note: minimal registration is required to download the free publications.)

http://www.ediscoverylaw.com/

A blog that is frequently updated discussing court decisions, new or modified laws, and other recent events relating to electronic discovery.
http://aiimknowledgecenter.typepad.com/weblog/2009/02/what-is-email-management.html

An online presentation on email management that covers many issues surrounding email management including business drivers for using email, concerns about privacy, legal issues and security issues, policy development, and email management technologies.