E-mail Management: A Guide For Harvard Administrators

E-mail is information transmitted or exchanged between a sender and a recipient by way of a system of connected computers. Although e-mail is considered a form of correspondence, it is not a discrete type of record. Instead it is a format in which information is transmitted and must be addressed on the basis of its informational content, rather than its physical form.

Is e-mail a record?

E-mail created or received as part of University business are University records and the property of the University. University records are defined in a vote of the President and Fellows dated March 13, 1995.

How do I take control of my office’s e-mail?

To ensure that accurate and authentic evidence of their business activities is preserved, and to assure ready access to needed information, University offices should establish and maintain clear and coherent policies and procedures for managing e-mail as records. Although in actual practice it will usually fall to each user to manage his or her own e-mail files - deciding whether messages are to be considered University records, and determining their importance and saving or deleting them - official policies and procedures are needed to guide them through the process. General guidelines for establishing policies and procedures are available in this document and in American National Standards Institute, ANSI/ARMA 4-2004, Requirements for Managing Electronic Messages as Records and ANSI/ARMA TR-02-2007, Procedures and Issues for Managing Electronic Messages as Records. The University Archives' Records Management Services is also available to assist offices.

What do I do to properly manage my office’s e-mail?

Like any other type of record, e-mail needs to be managed to ensure that it is secure, readily available when needed, accurate, kept as long as it is needed, and appropriately disposed of when it is no longer needed. It is the responsibility of each University office to ensure that its e-mail files are managed in a manner that meets the office's business needs for information, evidence and accountability, and that complies with University records management policies.

Offices should work with their information technology departments to ensure that:

- all staff are trained in use of the system and e-mail management
- there is complete and up-to-date documentation for the systems used to create, receive and maintain e-mail
- all appropriate security recommendations and requirements are being followed
- data and audit trails necessary to prove the system's reliability and use in the normal course of University business are retained
- complete systems backups are regularly and consistently performed and
- backup procedures are coordinated with disposition actions so that no copies of records are maintained after the retention period for the records has expired
What do I do to properly manage my office’s e-mail?

By its very nature, e-mail is not a secure medium for transmitting information. If confidential information is to be transported over a network, it must be encrypted.¹ Standard e-mail applications do not offer this level of security. For more information, see Harvard's Information Security and Privacy web site.

What are important considerations in composing e-mail messages?

Subject lines: Because of the high volume of e-mail, use a subject line that is short and descriptive of the subject of the e-mail. This will help your correspondents identify the incoming message and file and retrieve it for future use. Keep the subject lines consistent for all messages concerning a particular subject.

Addressees: Ensure that messages are only sent to those who need to receive them. Be especially careful when using:

- reply or reply-to-all functions
- automatically-completed e-mail addresses

Attachments: Managing e-mail attachments is difficult.

- Links between the attachment and the parent e-mail must be maintained
- Attachments usually are not searchable in e-mail clients
- Attachments cannot be read in the preview pane and require launching another application
- Attachments can be incompatible with the recipient's system
- Attachments are hard to read on portable devices
- Attachments take up a lot of space

If possible, use links instead of attachments and/or reference a file location on a shared drive. If it is necessary to send an attachment, it is helpful to include a description of it in the text of the e-mail to facilitate searching. When replying to a message containing attachments, remove the attachments unless they are required for a business purpose.

Signatures: Use a signature block to positively identify the sender.

How do I manage individual e-mail messages?

Both outgoing and incoming messages need to be managed and preserved to maintain a complete record of the office's activities. Outgoing messages are as important as, or perhaps more important than, incoming, and special care must be exercised to ensure that they are properly managed and retained.

Parts of a message: All e-mail messages will have at least three parts. The first two parts are the message's metadata. The first of these is the address or visible header, which appears at the top of all e-mails messages and includes the date and time the message was sent, the sender's identification, the subject of the message, and the existence of any copies or attachments. The second is the internet header which generally does not display in standard view and includes date-time stamps, transmission and routing data identifying the sending machine, addressee(s) and routing information, encryption information and other data. The third part of the e-mail is the message itself. Formatted attachments may also be appended to the message, or the message may have embedded links to pertinent resources. For a complete record, both the message, along with specific associated metadata, and any attachments or links need to be filed and preserved.

¹ Messages that need to be stored for a prolonged period should be unencrypted once they are entered into the record keeping system to ensure they can be retrieved and read in the future.
**Metadata**: The message’s metadata is what gives it context, and certain metadata elements must be preserved along with the message for as long as the message is retained. At a minimum, the following metadata elements in the visible header must be retained:

- The name of the sender
- The name of the primary recipient
- The name(s) of any other recipient(s) (this includes all members of a distribution list as well as cc’s)
- The date and time the message was sent
- Existence of attachments, if any

Additional metadata may need to be preserved based on the office's business needs. For example, if filing or reporting deadlines are critical, the date/time stamps for receipt of the messages and the computer IP address will need to be retained. Electronic signatures and encryption methods may also need to be retained. Offices should consult with Records Management Services and Office of the General Counsel to determine the level of metadata retention appropriate to their business functions.

When attachments accompany a message some form of reference must be provided that will maintain the connection between the message and the attachments.

**Identifying University Records**: Not all messages passing through a University e-mail system are University records and a significant proportion are likely to be non-University-record communications such as personal mail, spam or listserv traffic. Users need to be familiar with the definition of a University record and ensure that messages that are defined as University records are properly managed within the parameters of the office’s filing structure.

**Retention**: The value of an e-mail message is determined by its informational content. The length of time for which it is retained is based on its value to the University in conducting its business activities, complying with and fulfilling and ensuring its legal rights and obligations, fulfilling fiscal requirements, and in some cases documenting the history of the University. Always refer to the General Records Schedule or any special records schedule issued for your office for guidance. Although e-mail is treated like records in paper or other media in determining length of retention, the fact that e-mail is an electronic record may affect how or in what medium the record will be retained.

**How do I store my office’s e-mail?**

Long-term retention and access to e-mail is problematic. Generally speaking, e-mail systems are communication systems, not record keeping systems, and are not designed for the efficient management or preservation of messages stored on them. If e-mail is to be preserved for a long period of time, it must be removed from the e-mail system and entered into a record keeping system - either as hard copy or in electronic format.

E-mail is most effectively managed and stored in a records or content management system. However, even a basic e-mail repository will allow for the retention of a single official record that can be accessed by multiple users while ensuring its authenticity and accessibility over time.

As a general rule, the longer the message must be retained or the more it needs to be shared, the greater the need to remove it from the e-mail system and store it in some other manner - as hard copy, on the office's network, or in an electronic management system. Often there is no option to removing the e-mail from the system since IT departments may limit the space available to users to store their messages. The office should establish procedures for moving e-mail from individual users to the office filing system. If the e-mail and its attachments are stored electronically to meet business or retention requirements, care should be taken to ensure that the information is stored in a secure place, i.e. a drive that is regularly backed-up for disaster recovery.
Harvard does not at this time have the capability to preserve e-mail electronically for extended periods and e-mail needing long-term retention must be printed out. Although the sheer volume of messages makes printing e-mail problematic, and a printed message loses much of its information including metadata, hyperlinks and graphics, printing is currently the only strategy available for preserving the message over time.

Regardless of the storage method, the authenticity and integrity of the entire e-mail message must be preserved. That is, the records custodian must be able to attest that the e-mail is what it purports itself to be and that it has not been altered or corrupted. The original context must be described and an audit trail or chain of custody maintained for both the message itself and for any accompanying attachments or links. To ensure the continued authenticity and integrity of the message, the appropriate metadata must be identified and preserved along with the message itself (including attachments and embedded links). Offices must work closely with their IT departments to confirm that processes are in place to ensure that the metadata and message are not altered, and that they remain accessible and readable over their life span. The individual metadata elements that will need to be preserved in addition to those in the visible header may vary depending on whether the e-mail is to be preserved in electronic or printed format, and according to the office's business needs. Offices should consult with Records Management Services and the Office of the General Counsel to determine which elements to preserve.

**How do I e-mail that my office no longer uses?**

*Offices must make provisions to stop deletion of e-mail messages in the event of audit, litigation, investigation or other legal event.*

Disposition means that a record is removed from the custody of the office by transferring it to another office or to a University archives, or that it is intentionally destroyed. Any decision to retain or delete a record must be taken based upon the operational needs of the office consistent with University records policy and guided by applicable records schedules. Records that are scheduled for destruction should be eliminated as soon as possible after their retention period expires. Offices should contact their local archives program for guidance in transferring e-mail of historical value to the archives. At this time, all records transferred to an archives must be printed out along with the visible header information.

As with the disposition of any other University records, e-mail disposition should be regularized and documented. For e-mails printed to the files and those migrated to a record keeping system, this is not a difficult task, but if e-mails are to remain stored on the users' desktops, training programs must be instituted and procedures clearly defined in the office's procedures manual.

Users need to be made aware that there is a difference between deletion and destruction of any electronic record, e-mail included. Mere deletion or "trashing" of an electronic record does not result in its removal from the system. Generally, deletion merely frees up disk sectors for reuse, but the existing data may still be recoverable. It is also important to bear in mind that the trash barrels do not automatically empty. This must be done by the user, or the IT department must set the system to empty trash on a periodic basis. If this is how the trash is emptied, users must be aware that after a certain time they will be unable to readily recover anything that has been inadvertently deleted.

It is important for the individual offices to coordinate their destruction policies with their information technology departments. While the users in the offices may know what they need to keep or delete, they do not control the system and the IT personnel who do control the system have no real knowledge of the content and value of the records on it.

E-mail systems provide for a backup of messages that may be unaffected by user attempts to delete messages. Offices must be aware of back-up policies and coordinate with their IT departments to establish policies and procedures to ensure back-up tapes are identified and destroyed or reused on a periodic basis.
Secure deletion of University records is essential. Please refer to Harvard’s Information Security and Privacy web site.

When an employee leaves employment at Harvard, supervisory personnel should approve any deletion of e-mail. Any messages left behind in the employee's mailboxes that are University records must still be disposed of in accordance with records management policies.

**Should my staff be trained to manage their e-mail?**

Since most decisions regarding the management of e-mail will be made by the users, it is essential that the office put a training program in place. All office staff must be trained in using the e-mail system and how to identify, classify and manage the records they create and receive, and of the dangers improper use of the system may pose to the University. They must be made aware of proper retention and disposition procedures and of whom to contact when records need to be transferred out of their custody.

Upon request, Records Management Services will assist offices in developing and delivering training for their staff.