

Report for 11/03 meeting

Policies Reviewed

NOTE: I did not list policies that did not address retention or management of email (such as generic university email use policies).

- Mississippi Archives & Library Electronic Records Guidelines – no real answers, but a clear explanation of the problem
- University of Melbourne Managing your Electronic Mail – like question format; good disposition guidelines
- University of Delaware -- Good definition of legal issues and discovery
- Harvard University Archives: Electronic Records Management Guidelines – Good definition of “official records” for a public institution; some good filing examples, but too wedded to paper filing structures
- University of Washington Electronic Mail statement – short and to the point; great definition but little guidance
- University of Cincinnati Guidelines for Disposition of Electronic Mail – good, brief outline for disposition (six points)
- Ohio Electronic Records Committee – excellent policy manual, but not designed for a “general” audience; lots of great definitions and guidelines to use
- Utah Draft Electronic Records Policy – not in a very reader friendly format, but includes some good definitions as well as outlines the need for email system documentation
- Indiana Policy on Electronic E-Mail as Records – good, brief statement, but no policy at present
- University of Arizona Electronic Mail Policy – mostly about use regulations, not much about management
- Minnesota Historical Society Email Management – designed to help agencies develop policies, no specific guidelines
- North Carolina Email Guidelines – good question format but very lengthy
- Oregon State University Email Retention Policy – short and to the point! FAQ format

The portions I found best and/or most relevant follow. I also did not include a general “definitions” section beyond basic “email as record” statements, although I think that would be desirable in our overall guidelines. The excerpts are divided into eight sections.

1. DEFINITION OF UNIVERSITY RECORD

2. EMAIL AS RECORDS

3. CONSIDERATIONS WHEN CREATING EMAIL

4. DECISION PROCESS FOR MANAGING EMAIL

5. APPRAISAL OF ELECTRONIC RECORDS

6. DISPOSAL/RETENTION OF EMAIL/ELECTRONIC RECORDS

7. TECHNICAL/SYSTEMS CONSIDERATIONS

8. TRAINING FOR MANAGING EMAIL

Best Excerpts from Policies/Guidelines

1. DEFINITION OF UNIVERSITY RECORD

From Harvard Electronic Desktop Management Guidelines

<http://hul.harvard.edu/rmo/ElectronicDesktopManagementGuidelines.pdf>

Records are documents supporting the evidence of a business transaction and should be accessible, unchangeable, accurate, inviolate, and secure. "University records" [are defined] as recorded information, regardless of physical form or characteristics, created, received, used, recorded, or filed in the course of University business.

<http://hul.harvard.edu/rmo/emailguide.html>

University Records include all forms of recorded information regardless of physical characteristics, created, received, recorded, or legally filed in the course of University business or in pursuance of the University's legal obligations. These records serve as evidence of the University's organization, functions, policies, decisions, procedures, operations, or other activities. University records include but are not limited to minutes; correspondence; memoranda; financial records, such as invoices, journals, ledgers, purchase orders, and other information pertaining to fiscal matters, including grant fiscal matters; published materials, including reports and newsletters; moving images and photographs; sound recordings; drawings and maps; annotated copies or books; and computer data or other machine readable electronic records, *including electronic mail*. Records created or received by faculty in administrative and University committee capacities are also considered to be University records.

From Indiana University -- <http://www.indiana.edu/~libarch/ER/email-policy.pdf>

PURPOSE

The purpose of this policy is to establish an e-mail policy for all University departments and offices that create, use, and manage e-mail as part of the daily transaction of business.

SCOPE

This policy applies to all e-mail and e-mail attachments created or received by University personnel within the entire Indiana University system.

2. EMAIL AS RECORDS

From the University of Melbourne

<http://www.unimelb.edu.au/records/rmp/email.html>

ARE ELECTRONIC MAIL MESSAGES RECORDS?

A record comprises recorded information in any form, including data in computer systems, created, received and maintained by the University in the **transaction of business activities** or the conduct of affairs and retained as **evidence** of such activity.

Electronic mail created or received by University employees in connection with official business is a University record. Electronic mail messages are also records within the meaning of the Freedom of Information Act, the Public Records Act and are discoverable in litigation. They can be demanded under sub poena for production in court.

Electronic mail messages consist of three components :

1. Message Envelope (addressee, sender, date/time etc)
2. Message Body (text of the message)
3. Header Information (transmission details such as date & time of sending)

The integrity of the record relies upon these three components being maintained as a whole.

From University of Delaware <http://www.udel.edu/ExecVP/polprod/1-18.html>

While not all e-mail communications are records, all e-mail communications are subject to discovery and can be used as electronic evidence in the event of litigation. Discovery is the legal process that permits parties involved in a legal proceeding to obtain records and information relevant to the proceeding that are in the possession of another party. Unmanaged and unidentified e-mail records residing on University computers also pose a threat to the University's ability to document and reconstruct business and decision-making processes.

From the University of Washington
<http://www.washington.edu/admin/recmgt/uw.gs5.html>

- **Litigation.** Unless protected by legal privilege, email can and will be discoverable in litigation. This applies to email on disk or on a backup medium.
- **Legal Proceedings.** Like other forms of records, and regardless of retention requirements, email pertaining to pending audits, or judicial or public disclosure proceedings must not be destroyed until the issue is resolved.

From University of Arizona Electronic Mail Policy –
<http://w3.arizona.edu/%7Erecords/efinal.htm#appendixb>

WHAT YOU NEED TO DO (Storage of E-mail Documents)

Remember that in accordance with Arizona law, University business documents created or received on e-mail must be saved for the same length of time as their hard copy equivalents. There are two ways to comply with this:

- Create a folder in your e-mail account in which you save these messages. Back up your files appropriately; do not delete these messages. Save the e-mail message to your PC's hard disk as a file; or
- Print out a paper copy and save it in an appropriate file. In this case you do not need to save an electronic copy.

3. CONSIDERATIONS WHEN CREATING EMAIL

From the University of Washington

<http://www.washington.edu/admin/recmgt/uw.gs5.html>

- **Purpose.** Email is meant for informal correspondence and scholarly communications. It should not be used for official record-keeping purposes. (For further guidelines on the uses of email, see [Knowing the Rules](#) on the Computing and Networking page)
- **Privacy.** Confidential and sensitive information should not be sent via email. The privacy and integrity of an email message cannot be guaranteed. Also, once created, there is no guarantee that attempts to erase or delete email will be effective.

From the University of Melbourne

<http://www.unimelb.edu.au/records/rmp/email.html>

WHAT DO I NEED TO CONSIDER WHEN I CREATE AND SEND AN ELECTRONIC MAIL MESSAGE?

There are several actions that you can undertake in creating and sending electronic mail messages that will facilitate effective retrieval.

1. The first step is to identify whether the message you are sending is of short term facilitative value (eg. meeting arrangements, casual communications) or of continuing value. Messages of **continuing value** are those which :
 - approve or authorise actions or expenditure;
 - are formal communications between staff eg. correspondence or memoranda relating to official business;
 - signify a policy change or development;
 - create a precedent eg. by issuing an instruction or advice;
 - relate to the substantive business of the work unit or University;
 - involve negotiations on behalf of the University;
 - have value for other people or the work unit as a whole.

Messages of **short term facilitative value** are:

- distributed to a number of staff for information only eg news bulletins, circulars, meeting notices, copies of extracts of documents;
- drafts;
- created solely as part of preparation for other records;
- personal messages and announcements not related to official business.

2. Messages of continuing value should include keywords in the subject field as a means of identification and retrieval eg.
 - Budget
 - Admission
 - Training
 - Council
 - Security
3. The 'Confirmation of Receipt' function should be used if you require confirmation that the message has been received by the recipient and/or to document the accuracy and authenticity of messages. If this function is used the confirmation of receipt message should be printed and attached to the original message or linked to the original message electronically.
4. Before sending a message users should consider the need for formality. Formal messages often require a specific writing style eg. memorandums, agenda, circulars. Format and layout of messages aid comprehension of the information.

If the message is being circulated to a group it is advisable to name them at the beginning, Eg, To: Deans of Faculties

At the end of the text email users should specify the name and title of the author,
Eg:
Jan Smith
Records Manager

5. If the message is of continuing value include a file number at the beginning of the text. The file number may be for files held by Central Records, a Faculty Policy File or a work unit records system depending on the significance of the message.
6. Send and **print** messages of continuing value. Messages of short term facilitative value can be sent and deleted or stored in the email folders for future reference.

4. DECISION PROCESS FOR MANAGING EMAIL

From the University of Washington
<http://www.washington.edu/admin/recmgt/uw.gs5.html>

Email is managed by its content, not its format.

From Ohio Electronic Records Committee –
<http://www.ohiojunction.net/erc/email/emailguidelines.html>

The management of e-mail systems touches on nearly all functions for which a government agency is dependent on recordkeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to manage e-mail messages and systems properly, then, is the same as for other records keeping systems -- to ensure compliance with Ohio laws concerning the creation of, retention of, and access to public records.

Government agencies that use electronic mail have an obligation to make employees aware that e-mail messages, like paper records, must be retained and destroyed according to established records management procedures. Agencies should set up or modify e-mail systems to facilitate electronic records management. Procedures and system configurations will vary according to the agency's needs and the particular hardware and software in place.

From Indiana University -- <http://www.indiana.edu/~libarch/ER/email-policy.pdf>

The effective management of e-mail is one of the primary objectives of IU's records management program. E-mail messages may qualify as business records, and in some cases, may be the only record created that documents a transaction, an action taken, or a policy determination or interpretation. It is therefore extremely important that all University personnel recognize the significance of the e-mail messages they create or receive and manage them properly.

From Mississippi Division of Archives and History
<http://www.mdah.state.ms.us/arlib/ergleml.html>

1. **Archiving by individual decision.** The decision of what to discard and what to archive can be left entirely to the individual employee. All email would be downloaded to the desktop, employees could file messages for retention (including copies of outgoing messages) in appropriate folders, and they could then copy the folders to a server designated to receive archival materials at regular intervals, from which the records could be transferred directly to the archives. Such a practice would require extensive employee training and explicit employee awareness of their recordkeeping responsibilities; it would also require considerable trust in employees and confidence in their technical abilities and the maintenance of their computer equipment.
2. **Individual decision plus partial automation.** Incoming email can be captured on the server using appropriate filters developed in collaboration with records officers to meet retention requirements. Employees can be asked to tag outgoing email, using the subject line, in such a way as to indicate its retention status and the archival series to which it should belong. Some specific syntax should be used for this, such as:

[Work] [series]
standard message title

Alternatively, employees could tag outgoing email for what should NOT be retained: for example, a [Personal] or [Private] tag, instead of a [Work] tag, could be used. Some agencies have expressed opposition to the idea of allowing people to tag things privately, as that may imply that the agency condones the use of the computer and its resources for private purposes. Whatever is done, it will require considerable trust in employees and confidence in their abilities. It must be explicitly documented and must involve the training of every employee in what should or should not be tagged. It should be said that at least one specific study has shown that employee tagging is not very effective in practice unless it is routinely reviewed by supervisors.

3. **Automated archiving.** At the mail server level, all incoming and outgoing email that is of interest can be saved using specifically-designed filters to exclude that which is not of interest. Incoming email is easier to manage, since commercial advertisements ("junk" email) and email coming from listservs that are likely to be archived elsewhere can easily be excluded. Outgoing email is far more difficult. In the first place, although incoming email

may not initiate or further official business, outgoing email in theory is all for official business: much official correspondence travels via email, and even outgoing mail addressed to listservs may represent the agency to a large audience of professionals, just as would a printed letter to the editor. Although it should be possible to devise filters for outgoing email that scan for certain text strings, certain senders, etc., it may simply be less complicated to preserve all outgoing (and incoming) email for transfer to the archives, leaving any filtering, discarding, or marking of materials to occur after transfer instead of before and placing the responsibility of determining what is archival on the archivists, as is often now done with many paper records.

5. APPRAISAL OF ELECTRONIC RECORDS

From Utah State Archives --

<http://www.archives.state.ut.us/recmanag/electronicpolicy.htm>

5.2.1 High-risk records: These are records whose loss would pose a significant fiscal, legal, or administrative risk to an agency if they could not be accessed or read for the entire length of their retention. These records will be managed according to the Archives' [Procedures for Managing High-Risk or Permanent Electronic Records](#).

5.2.2 Medium-risk records: These are records whose loss could pose a fiscal, legal, or administrative risk to an agency if they could not be accessed or read for the entire length of their retention, but agencies have discretion in weighing resources vs. business need. Choice of storage media may contribute to the degree of risk. These records should be managed according to the Archives' [Procedures for Managing Medium-Risk Electronic Records](#).

5.2.3 Low-risk records: These are records whose loss would pose limited fiscal, legal, or administrative risk to an agency if they could not be accessed or read for the entire length of their retention. These records should still be managed, but choice of storage media and the timetables for testing and replacing media will be left to discretion of the agency as resources allow.

6. DISPOSAL/RETENTION OF EMAIL/ELECTRONIC RECORDS

From Oregon State University --

<http://extension.oregonstate.edu/ectu/tech/Handouts/Emailretention.pdf>

How long do I need to keep e-mail messages?

When e-mail messages are filed as part of the documentation supporting an agency program or function, they have the same retention as the records they are filed with. Typically, e-mail messages pertain to an agency program or function and they should be filed with the records supporting the program or function. E-mail messages may be filed as one of the various categories of correspondence only when they do not relate directly or obviously to an agency program or function. When they are filed as correspondence, you may use the retentions contained in OAR 166, Division 300 (the Archives Division General Schedule).

These retentions are:

Administrative Correspondence (5 years)

Fiscal Correspondence (4 years)

General Correspondence (1 year)
Ephemeral Correspondence (Retain until read, destroy)

From the University of Melbourne
<http://www.unimelb.edu.au/records/rmp/email.html>

Checklist for disposal of electronic documents

1. Does this message grant some kind of approval under a delegated authority e.g. authorise the expenditure of funds?

If yes, print, have it signed by the authorising officer and file as indicated in the message. (All such messages should indicate where a signed copy will be filed).

2. Does this message:
 - o signify change in policy ?
 - o create a precedent ?
 - o relate to the substantive business of the work unit, section or university ?
 - o include legal advice ?
 - o involve negotiations on behalf of the University ?

If yes to any of the above, print & file in Central Records

3. Is this a formal communication between officers?

If yes, print & file in work unit or Central Records

4. Is the message used to initiate, continue or complete a departmental activity?

If yes, print & file in work unit or Central Records

5. Does the message have continuing value for others in the work unit?

If yes, print & file in the work unit

6. Does anyone external to my work unit need to be aware of, or refer to, this message in the future?

If yes, print & send to Central Records

7. Are there other messages on this matter ie. answers and responses, prior messages?

If yes, evaluate them together

8. Is the message of information value only eg. an information copy?

If yes, delete the message

9. Does the message comprise draft information leading to a final version?

If yes, delete the message

10. Is the message of short term facilitative value eg. arranging a meeting?

If yes, delete the message

11. Does a paper copy exist?

If yes, delete the message

From the University of Cincinnati

<http://www.archives.uc.edu/recmgmt/>

Electronic mail created and received by employees of the University of Cincinnati during the course of business is an official University record, and as such falls under the purview of the University Records Management Program. Additionally, the University's computing resources are limited physically and financially in the amount of online storage which can be provided to users with electronic mail accounts. For both of these reasons, the following guidelines are important in ensuring effective, efficient and legal retention and disposition of electronic mail.

1. Retain delivery and read receipts only if legally required. Generally these should be deleted and purged once they have been read.
2. Delete and purge all junk mail once read. If there is anything a user feels will be of later use, it should be printed and filed as hard copy.
3. Delete and purge C.I.T.S. systems notifications once they have been read.
4. Print and file routine correspondence and inter-office memoranda and retain until no longer administratively useful. Purge and delete electronic copies.
5. Print out and file executive correspondence, that of administrators with the rank of Department Head and above and Faculty. Such correspondence documents administrative decision-making, committee, faculty, and campus activities and is retained in hard copy for 3 years or until no longer administratively useful, and then transferred to the University Archives. Electronic copies should be deleted and purged daily or weekly, depending upon the volume of use.
6. Faculty correspondence, research data, and external scholarly communications (for example through the Internet) which are not of an administrative nature may still have significant archival value. These are printed out and filed with the Faculty member's papers. Electronic copies should be deleted and purged daily or weekly depending upon the volume of use.

7. TECHNICAL/SYSTEMS CONSIDERATIONS

From Utah State Archives

<http://www.archives.state.ut.us/recmanag/electronicpolicy.htm>

5.2.4 Documentation: Agencies are encouraged to maintain adequate and up to date technical documentation for each electronic information system that produces, uses, or stores long-term data files. Recommended documentation is the following:

- (a) A narrative description of the system;

(b) Physical and technical characteristics of the records, including:

(i) A record layout that describes each field including its name, size, starting or relative position, and a description of the form of the data (such as alphabetic, zoned decimal, packed decimal, or numeric), or

(ii) A data dictionary, or

(iii) The equivalent information associated with a data base management system including a description of the relationship between data elements in data bases; and

(c) Any other technical information needed to read or process the records.

8. TRAINING FOR MANAGING EMAIL

From the Minnesota Historical Society --

<http://www.mnhs.org/preserve/records/electronicrecords/eremail.html>

Staff members will need to be trained on how to answer legal and operational questions about e-mail. Your training and documentation material should set forth guidelines that staff members can follow to answer such questions in the course of their work. Possible questions include:

- Is this e-mail an official record? Is this e-mail message administrative or personal (e.g., "Thursday staff meeting to start an hour late." or "Let's do lunch!")?
- Does this e-mail message have long-term significance (e.g., "New policy finalized.")? Does this e-mail message document a transaction or operations function (e.g., a process, a decision, or a discussion)?
- Is this e-mail record public or not-public as set forth by the MGDPA?
- What metadata must I capture when I save this e-mail record?
- Which records series does this e-mail record belong in?
- Should I save the complete e-mail record, including attachments and group list names
- Could this e-mail message ever be required as evidence in a legal action?