Digital Records Pathways:
Topics in Digital Preservation

Module 6: Email Management and Preservation

InterPARES / ICA
DRAFT July 2012

Table of Contents

Digital Records Pathways: Topics in Digital Preservation

1 Preface

Digital Records Pathways: Topics in Digital Preservation is an educational initiative developed jointly by the International Council on Archives (ICA) and the International Research on Permanent Authentic Records in Electronic Systems Project (InterPARES). It offers training to archivists and records professionals in the creation, management and preservation of authentic, reliable and usable digital records. The program assumes that the user has a solid grounding in basic concepts of records management and archival theory, and builds on that knowledge.

Consisting of eight independent modules, *Digital Records Pathways* addresses the theoretical and practical knowledge needed to establish the framework, governance structure and systems required to manage and preserve digital records throughout the records' lifecycle.. Each module addresses a specific topic of relevance to the management and preservation of digital records. The program is provided free of charge on the ICA website at www.ica.org/.

1.1 About the ICA and InterPARES

The ICA and InterPARES are committed to establishing educational materials for the continuing education of archivists and records managers, to build upon foundational knowledge, disseminate new findings, and to equip archivists and records professionals with the necessary specialized knowledge and competencies to manage and preserve digital records.

The International Council on Archives (ICA) (www.ica.org) is dedicated to the effective management of records and the preservation, care and use of the world's archival heritage through its representation of records and archives professionals across the globe. Archives are an immense resource. They are the documentary by-product of human activity and as such an irreplaceable witness to past events, underpinning democracy, the identity of individuals and communities, and human rights. But they are also fragile and vulnerable. The ICA strives to protect and ensure access to archives through advocacy, setting standards, professional development, and enabling dialogue between archivists, policy makers, creators and users of archives.

The ICA is a neutral, non-governmental organization, funded by its membership, which operates through the activities of that diverse membership. For over sixty years ICA has united archival institutions and practitioners across the globe to advocate for good archival management and the physical protection of recorded heritage, to produce reputable standards and best practices, and to encourage dialogue, exchange, and transmission of this knowledge and expertise across national borders. With approximately 1500 members in 195 countries and territories the Council's ethos is to harness the cultural diversity of its membership to deliver effective solutions and a flexible, imaginative profession.

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) (www.interpares.org) aims to develop the knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form and provide the basis for standards, policies, strategies and plans of action capable of ensuring the longevity of such material and the ability of its users to trust its authenticity. The InterPARES project has developed in three phases:

InterPARES 1 (1999-2001) focused on the development of theory and methods ensuring the preservation of the authenticity of records created and/or maintained in databases and document management systems in the course of administrative activities. Its findings present the perspective of the records preserver.

InterPARES 2 (2002-2007) continued to research issues of authenticity, and examined the issues of reliability and accuracy during the entire lifecycle of records, from creation to permanent preservation. It focused on records produced in dynamic and interactive digital environments in the course of artistic, scientific and governmental activities.

InterPARES 3 (2007-2012) built upon the findings of InterPARES 1 and 2, as well as other digital preservation projects worldwide. It put theory into practice, working with archives and archival / records units within organisations of limited financial and / or human resources to implement sound records management and preservation programs.

1.2 Audience

The audience for this program includes archivists and records and information professionals interested in expanding their competencies in the management of digital records. Taken as a whole, the modules form a suite of resource materials for continuing professional education with particular focus on issues influencing the preservation of reliable, accurate and authentic digital records.

1.3 How to Use the Modules

Each module consists of theoretical and methodological knowledge and its practical application, illustrated through case studies and model scenarios. While the modules have been developed by InterPARES Team Canada, and are therefore illustrated with examples from the Canadian context, each module is customizable for a specific domain or juridical context. For wider applicability, they have been translated into the languages of the ICA partners.

The modules can be studied individually according to need and interest, or as a set, covering the range of competencies required. They can be self-administered by individuals, or offered through professional associations or workplace training. The modules also contain a number of templates that allow universities and professional associations to adapt and to develop specific course curricula, on-site training materials for students and professionals on digital recordkeeping and preservation issues. Universities and professional associations are free to adapt the materials and develop their own context-specific course curricula and training kits.

1.4 Objectives

The modules have the following objectives:

- To provide educational resources based on cutting edge research in digital records issues to professional archival and records management associations for the benefit of their members;
- To provide archivists and records managers with the necessary theoretical knowledge as well as procedural and strategic skills to develop, implement and monitor a digital recordkeeping and/or a preservation program;
- To illuminate theoretical concepts with practical applications through real life examples drawn from case studies, anchored in specific administrative and technological contexts;
- To provide university programs with content and structure for courses on digital records management and preservation.

1.5 Scope

Digital Records Pathways: Topics in Digital Preservation consists of the following modules:

Module 1: Introduction – A Framework for Digital Preservation
Module 2: Developing Policy and Procedures for Digital Preservation
Module 3: Organizational Culture and its Effects on Records Management Selection and Appraisal of Digital Records
Module 4: An Overview of Metadata
Module 5: From *Ad Hoc* to Governed – Appraisal Strategies for Gaining Control of Digital Records in Network Drives
Module 6: E-mail Management and Preservation
Module 7: Management and Preservation of Records in Web Environments
Module 8: Cloud Computing Primer

Each module consists of some or all of the following components as appropriate:

- **Overview** of the topic and scope of the module;
- **Learning objectives** and expected level of knowledge upon completion;
- **Methodology** or the procedures to follow in order to apply the module;
- **Templates (where appropriate)** to facilitate the implementation of the module;
- **Case Study(ies)/Scenarios (where appropriate)** that provide real-world examples of module topic
- **Exercises** covering key learning points;
- **Review questions** to enhance comprehension and understanding of the topic;
- Additional **Resources** for the topic, including **readings, standards** and other **templates** for reference

Overview of the set			
1. A Framework for Digital Preservation 2. Developing Policy and Procedures for Digital Preservation			Foundational
3. Organizational Culture	4. An Overview of Metadata	5. Appraisal Strategies	General purpose
6. E-mail	7. Websites	8. Cloud Computing	Specific purpose
International Terminology Database			Foundational

1.6 International Terminology Database

The terminology used in the modules reflects common usage in archival and records management communities of practice. To ensure common understanding, and minimize potential confusion that may arise from regional or jurisdictional practice, all modules are supported by the International Terminology Database, available at http://www.web-denizen.com/. As well, certain specific terms are included in short glossaries in each module.

Module 6: E-mail Management & Preservation

2 Introduction

Managing and preserving electronic mail (e-mail) has become a formidable challenge for most organisations. There have been some estimates that over 100 billion e-mails are created worldwide every day, with some predicting that this number may double within the next five years.[1] The deluge of e-mail has, in many instances, threatened to paralyze organisations and work productivity.[2] In today's fast-paced digital world, failing to properly manage and preserve e-mail may have severe consequences for an organization, such as loss of worker productivity, loss of clients or retailers, or litigation. Organisations that successfully manage and preserve the myriad amounts of incoming and outgoing messages should be able to function more effectively and efficiently and better protect themselves against legal risks while ensuring the preservation of their corporate memory.

An e-mail should not be considered any different from any other type of electronic record. E-mail should be managed alongside all other organizational records, that is, it should be classified and applied to retention and disposition schedules. However, many organisations lack the resources (e.g., financial, technological) to manage e-mails with other electronic records.

This module is designed to help you gain better control of your organization's e-mail. The module walks you through a series of steps that will facilitate the implementation of new policies, procedures, and practices with regards to how staff manage and preserve their electronic messages.

The module is divided into 6 sections. **Section 1** includes general information about the module – its aims, objects, and intended learning outcomes – as well as terms and definitions specific to the module. **Section 2** reviews the E-mail Management and Preservation Model (EMPM). This is the most comprehensive section of the module as it reviews each phase of the process. **Section 3** provides an example of a case study that uses the EMPM. **Section 4** contains a sample e-mail guideline that is referenced in Section 3. **Section 5** is a review section that poses a series of review questions about the module's content. This section aims to reinforce the key components of e-mail management and preservation. Additional exercises are also intermixed with the text; these questions are different from those found in this section. **Section 6** provides additional resources and information about e-mail management and preservation. **Appendix A** and **Appendix B** complete the module. Appendix A is a worksheet that may be used when collecting contextual information about the organization, and Appendix B

---

[1] Sara Radicati, "Email Statistics Report, 2012-2016." The Radicati Group, Inc. (10 April 2012): http://www.radicati.com/?p=8262. See also "Worldmeters: Real Time World Statistics," available online at http://www.worldometers.info/.

[2] Bill Tolson, "Email Overload Costing Organizations Time and Money," Iron Mountain (6 December 2010): http://blog.ironmountain.com/2010/uncategorized/e-mail-overload-costing-organisations-time-and-money-new-study-shows-that-1-in-5-uk-workers-spend-32-days-a-year-managing-their-e-mail/.

is a same questionnaire that may be used when gathering information about how employees manage their attachments.

2.1 Aims and Objectives

The objective of this module is to explain the e-mail management and preservation model (EMPM), a multi-phase process for implementing e-mail management and preservation policies and procedures. This module will discuss the various factors that influence e-mail management and preservation, different e-mail management methods, ways to apply retention and disposition to e-mail, ways to preserve e-mail, and the design and implementation of e-mail policies and procedures.

2.2 Learning Outcomes

Upon completion of this module, you will be able to:

- Understand the key issues involved in the management of e-mail;
- Understand the key issues involved in the preservation of e-mail;
- Understand different strategies for managing e-mail;
- Understand different strategies for preserving e-mail;
- Know where to locate additional information and resources that will facilitate how you manage and preserve e-mail in your organization.

2.3 Terminology

This section identifies and defines key concepts/constructs that are used throughout this module.


See the ICA International Terminology Database at www.web-denizen.com for more terminology relevant to this module.

Administrative or Working File E-mail: Messages relating to the general and routine activities of the unit.

Attachment: A document that accompanies, or is "attached," to an electronic message; attachments may appear in almost any format and be any size.

Discovery/Disclosure: The process of identifying, locating, securing, reviewing, and producing potentially relevant information and materials during the course of legal action.

Directory of records (DOR): A tool used by many records management programs that provides a global view of the records generated by a specific organization and divides this view into a classification scheme consisting of a set number of broad sections of related records.

Electronic mail (e-mail): A document created or received via an e-mail client; this data includes the header information, text body, metadata, and any attachments that accompany the message. Also known as an electronic message.

E-mail client: The e-mail software or program used to receive or send electronic messages; ex. Microsoft Outlook, Eudora, Microsoft Mail, Gmail, Hotmail.

E-mail management: Creating, receiving, sending, classifying, or destroying an e-mail.

E-mail preservation: The specific process of maintaining e-mails during and across different generations of technology over time, irrespective where they reside.

Transitory e-mail: An e-mail that has little or no documentary or evidential value and that need not be set aside for future use.

3 E-Mail Management and Preservation Model (EMPM)

The E-mail Management and Preservation Model (EMPM) consists of four phases: Identification; Determination; Design; and Implementation (Figure 1).

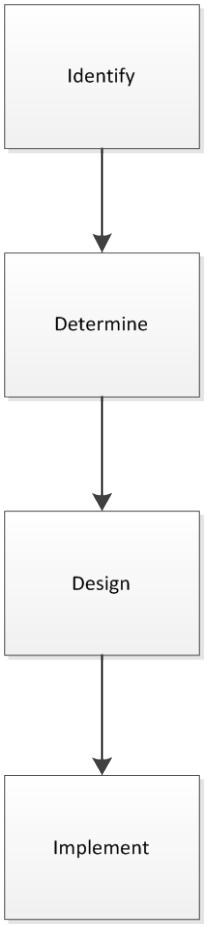

Figure 1: E-mail Management & Preservation Model (EMPM) – Simplified

As shown in Figure 2, these phases expand into the following processes:

1) Identifying contextual factors that influence the management and preservation of e-mail;
2) Determining the best ways to manage and preserve e-mail within the organization;
3) Designing or revising e-mail management and preservation policies and procedures; and
4) Implementing e-mail management and preservation policies and procedures.

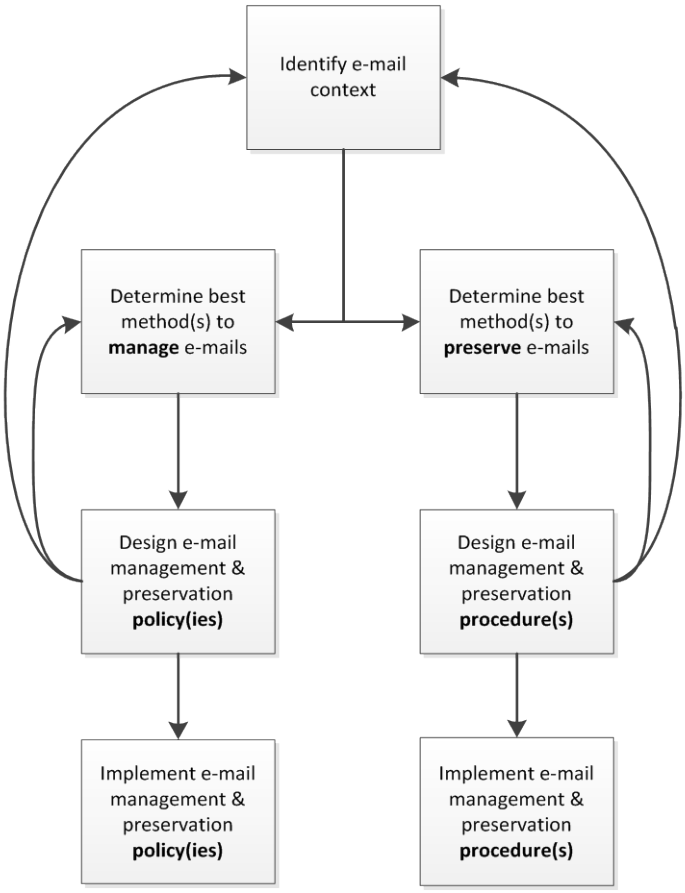

Figure 2: E-mail Management & Preservation Model (EMPM) – Expanded

As depicted in Figure 2, the EMPM consists of a series of steps, some of which may be reiterative or occur concurrently with other steps. For example, Steps 2 and 3, identifying internal and external factors and determining the best ways to manage and preserve e-mails do not need to be completed in order, but in some situations the contextual information acquired during these phases may be necessary before proceeding to the next stage. All information should be obtained and all policies and procedures should be designed prior to implementation.

The following subsections guide you through each of these phases, providing you with the information you need to satisfy their requirements and be able to move to the next step.

3.1 Identify E-mail Context

This may be one of the most time-consuming and cumbersome phases of the EPMP, but its importance cannot be underestimated. Prior to devising any new strategies or implementing any new guidelines or procedures for e-mail management and preservation, you must first evaluate how e-mail is managed and preserved at your organization. This information will most likely be obtained by meeting with as many of the relevant stakeholders as possible, such as senior administrators, legal counsel, IT, and other staff members that create and manage e-mail. As shown in Figure 3, there are several contextual factors that must be taken into consideration: Records Management Principles; Technological Capabilities; Organizational Culture Tendencies; and Legal Issues. Understanding these factors will ensure that your implementation strategies are realistic and practical given your organization's resources and working environment.

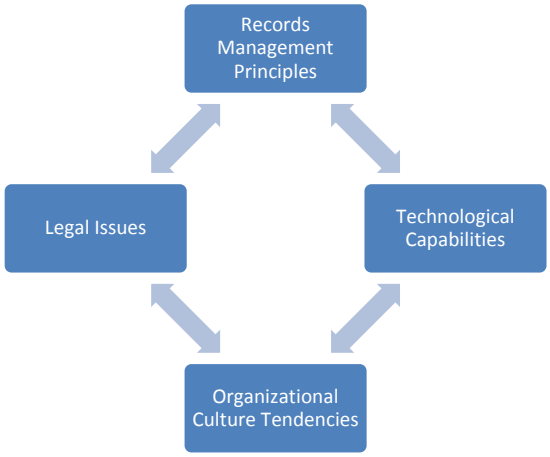

Figure 3: Contextual Factors of E-mail

3.1.1 Records Management Principles

As your organization's records professional, you should already be aware of the records management principles and practices currently practiced at your organization.[3] This module, and the others that accompany it, offer an opportune time for you to review the effectiveness of these practices and the currency of any accompanying documentation.

---

[3] For example, see section 7.1, Records Management Requirements, from ISO 15489-1, "Information and Documentation—Records Management—Part 1: General," Geneva, Switzerland: International Organisation for Standardization, 2001.

For example, you may want to revisit retention and disposition requirements for some records series; update policies and procedures related to records management functions; or reconsider the strengths and weaknesses of any educational tools, presentations, or documents you use to instruct employees about the importance of records management or records management practices.

3.1.2 Technological Capabilities

The management and preservation of e-mail primarily relies on the technological capabilities of the organization. Within any organization, there are a number of technological features that should be considered when evaluating e-mail management; these include but are not limited to:

- E-mail client-server applications (e.g., MS Outlook, Pegasus Mail, Eudora, Thunderbird, Apple's Mail, etc.;
- Communication protocols (e.g., POP, IMAP, SMTP, LDAP);
- Hardware server space allocations and availability;
- Duration that e-mails are kept in digital trash bins;
- Users' inbox quotas;
- Backup capabilities and practices;
- Computer hardware system(s) and software products being used;
- Other digital devices being used by employees (e.g., Blackberries, iPhones, tablets, etc.);
- Information/records management systems being used (e.g., EDRMS, ECM, shared network drive or local area network, etc.).

3.1.3 Legal Issues

Similar to the technological issues, legal issues are contextually based and depend on the location and jurisdiction of the organization. Like most other digital records within your organization, e-mail must be applied or be managed in compliance with national, regional, or local laws and regulations, which may include legislation pertaining to:

- Access to information;
- Archives legislation;
- Laws of evidence and rules of court;
- Privacy and personal information protection;

- Laws, regulations, or ordinances relating specific to your organization's business environment (e.g., pharmaceutical industry).

The legal context should include any applicable or relevant policies, guidelines, or procedures created by the organization that employees must adhere to, such as a records management policy, use of information technology policy, or e-mail guidelines.

Conducting a risk assessment of your organization's legal environment may influence which area(s) of your organization you approach first to implement new strategies for managing and preserving messages. For example, some records, such as those produced by Human Resources, Accounting, or Research and Development may be in higher demand when facing Access to Information requests or orders to produce records for litigation. Likewise, e-mails in the possession of senior management or their assistants may be requested more frequently than the messages of other employees. It is important to identify the areas within your organization that may be in greatest need of improved e-mail management and preservation practices to ensure that messages are properly retained and disposed and not erroneously destroyed.

3.1.4 Organizational Culture Tendencies

There are a variety of organizational factors that should be considered when evaluating e-mail management and preservation plans. Understanding the role e-mail has within the organization, how it is used, and perceived by its users will facilitate the implementation of any new policies or procedures.

See Module 3: Organizational Culture and its Effects on Records Management for more information

First you must know which, if any, organizational policies and procedures already apply to e-mail management and preservation. If they already exist, do they need to be updated to reflect changes within the organization (e.g., from the introduction of new technology or the creation of new functions that result in new records), or changes external to the organization (e.g., the implementation of new laws or regulations)?

In many organisations, e-mail is used for a variety of purposes. By conducting workflow and work process analyses, you will gain a better understanding of the roles that e-mail serves in your organization. This analysis will provide some indication why employees create, send, and receive e-mails – information vital to understand how users may respond to new or revised records management policies and procedures that address e-mail management. To further facilitate the implementation of these documents, it will also be helpful to know if, how, or when employees:

- manage e-mails;
- save e-mails;

- handle e-mail attachments; and
- delete e-mails.

Managing E-mails

Depending on the technological resources of your organization, employees may manage their e-mails in one of three different ways. They may opt for the "no classification" approach, that is, leave most, if not all, of their messages in their Inbox and Sent folders. Another option may be that the employee prefers to create a folder classification structure and file messages according to an individual- or enterprise-designed or scheme. If the organization uses an EDRMS and it is connected to the e-mail client, employees may rely on this system to manage their messages rather than their e-mail client. It is also possible that the employee uses a combination of all three methods. Section 2.2.1 discusses the strengths and weaknesses of these methods.

Saving E-mails

Depending on the technological infrastructure of the organization, most employees will leave their messages in their e-mail client—either in the inbox or a folder classification structure. Aiming to facilitate access to messages or safeguarding them against destruction, employees may prefer to save their messages to locations external to their e-mail client, such as on their desktop computer, the organization's server space, or other portable storage media (e.g., thumb drives). Saving e-mails to other locations may have several detrimental effects on the organization such as hindering the fulfillment of access to information requests, preventing the retrieval of relevant records during the discovery/disclosure process of litigation, or simply create unnecessary duplication. Section 2.2.1 discusses some best practices for how e-mails should be saved external to an e-mail client.

Handling Attachments

E-mail attachments function as an integral component of any message. An authentic e-mail is one that contains its full text (including header information), any attachments, and all metadata associated with that message. In some legal jurisdictions, there may be legal ramifications if an e-mail is found not to have its attachment accompany it to court—consequences that may include financial penalties early in the legal process, the record not being admitted as evidence, or the record be given a reduced amount of legal weight.

There are a variety of ways by which an attachment may be downloaded or saved to another location; these methods may be dictated by the e-mail client. In many cases, an attachment will remain intact with the original message if the e-mail is retained. It is important to keep track of where employees download their attachments and how they name the new file in order to maintain the relationship to the associated e-mail. Moreover, some e-mail clients allow a user to remove or delete the attachment from an e-mail (Figure 4); oftentimes, this may be done to reduce the message's size and, subsequently, save server or inbox quota space. Appendix B provides a preliminary set of questions that may be asked when inquiring about attachment management. Section 2.2.1 discusses some best practices for how e-mail attachments should be handled.

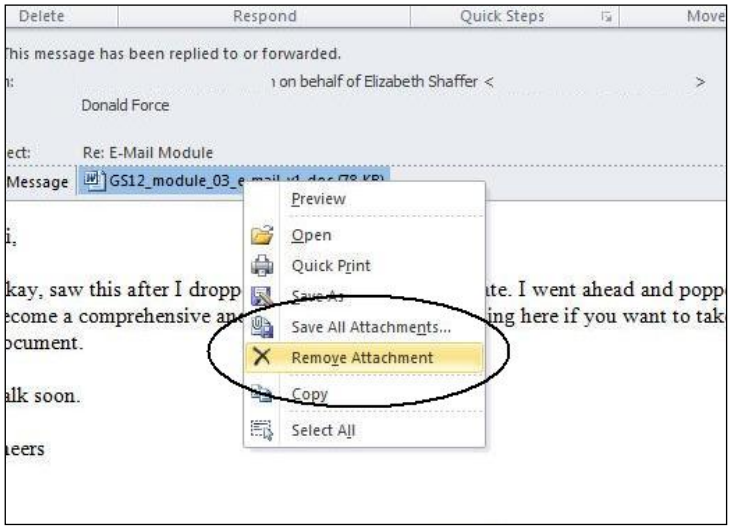

Figure 4: Remove Attachment Option (Outlook). This feature appears when right-clicking on the attachment.

Deleting E-mails

One of the greatest challenges associated with managing e-mail is dealing with its volume. For every message that is created, two or more may be received. Oftentimes, employees may feel so overwhelmed by the number of messages, coupled with their daily tasks, that they lack the ability to destroy e-mails. It is not uncommon for users to save everything simply because it is easier to do. You need to make sure messages are deleted in accordance with your organization's disposition schedules. Section 2.2.1 discusses some strategies for applying e-mails to retention and disposition schedules.

Exercises:

1. What are some of the laws and regulations that apply to your organisation?
2. What organisational documentation applies to current e-mail management and/or preservation use at your organisation? Where might a new policy e-mail management and/or preservation fit within your organisation?
3. As an employee of your organisation, how do you manage your incoming and outgoing e-mails?

3.2 Determining Best Method(s) to Manage E-mails

Once the contextual information about e-mail has been obtained, the next phase is to determine the best way(s) that you believe e-mail should be managed. You must keep in mind that there may not be one total solution for all the departments or employees at your organization, but every attempt should be made to ensure that employees manage their messages consistently and according to best practices. Since every organization's contextual situation is different (and may even vary between units), this module does not advise you how e-mail should be managed; rather, it aims to provide you with options that you may carry forward to address the challenges your organization faces.

3.2.1 Management Methods

As mentioned in section 2.1.4, there are three primary methods for managing e-mails: no classification, classification structure, or EDRMS. These methods may vary depending on the organization's technology and the e-mail user's personal preferences. Some employees will diligently and meticulously organize their messages into an elaborate classification scheme, while others will rely on their inbox to hold all their messages. For some organisations, e-mail will be retained and managed in an EDRMS, which may negate the personal use of an e-mail client. In some organisations, a combination of all three methods may be used. Regardless of which method(s) is/are used, no one method is perfect and they all have their strengths and weaknesses.

No Classification

It is widely acknowledged that many people tend to relegate their messages to only a few locations within the e-mail client, most often, their inbox, sent folder, and a small number of other folders created as a result of their day-to-day needs. One benefit of this method is that all messages may be confined to a few locations, thereby reducing the amount of time browsing complex folder hierarchies. This approach is often supported by the argument that the e-mail client's search capabilities suffice for retrieval, thereby negating the need for an elaborate folder hierarchy. Despite even the best search engines, as the volume of messages increases within the few folders, effective recall will become increasingly difficult and result in the user spending more time browsing through longer lists of search results. Moreover, leaving messages in only a few locations makes it a challenge to properly apply retention and disposition schedules to messages.

Classification Structure

Folder classification may develop in several ways:

1) By the user as a result of his/her job duties and functions.
2) By the records professional as part of the organization's EDRMS.

3) By the records professional for the user or specific area of the organization (e.g., department or unit).

Regardless of the impetus behind a folder classification scheme, the structure may help establish the context of the e-mail message because the folder names (if properly labeled) may identify the functions and duties of the user's position. A folder classification scheme may facilitate the retrieval of e-mails by limiting the number of messages that a user must sort and browse. E-mail classification may also help records professionals apply retention and disposition schedules to e-mails if the folders are established by job function and in accordance to the organization's schedules. Folder structures are not perfect. Of course, there is no guarantee that users will always properly file their messages. These hierarchies need to be revised as job functions change. There may be a threshold limit to the usability of a folder structure – too many folders and too many levels may limit the user's ability to effectively and efficiently classify e-mails.

With certain e-mail clients, the classification of e-mail into a folder structure may be facilitated by the creation of "Rules." These rules enable the e-mail client to automatically move a message into a designated folder depending on specified conditions, such as the sender's name or e-mail address, specific words in the subject line or message body, the intended recipient's name or e-mail address, or the message's sensitivity or level of importance (Figure 5). Using Rules is not without its limitations. For example, establishing a rule may be a lengthy process of trial-and-error as it takes time to fine-tune to the rule to capture all intended messages. In other words, rules may be used best in narrow, highly regimented business practices, where elements of the messages (i.e., sender, subject line, text in the body, etc.) are consistent over time. Furthermore, when a rule is engaged, it is up to the user to check regularly the designated folder(s) to ensure that all received messages are acknowledged, read, and responded to as necessary.

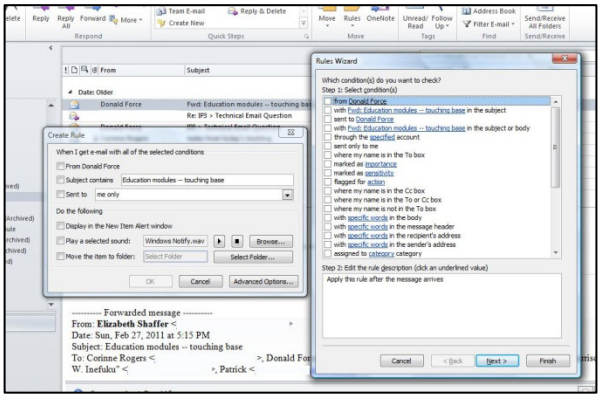

Figure 5: E-mail Rules (Microsoft Outlook)

Electronic Document and Records Management System (EDRMS)

Organisations requiring users to move e-mails into an EDRMS have the advantage of managing and preserving e-mails alongside the their other digital records. An EDRMS

may facilitate recall if users are able to effectively interact with the system. Some applications have the built-in capability to seamlessly integrate a variety of traditional applications (such as MS Office products), though other systems may need to be adjusted to ensure proper functionality. For example, some systems may convert e-mail attachments to another format and/or save it in a separate location from the e-mail it accompanied. Also, depending on the relationship between the system and the e-mail client, employees may need to be instructed to delete the original message from their e-mail client once it has been migrated to the EDRMS, though, in many cases, organisations may set the system to automatically delete messages from the e-mail server after a specific period of time, such as 30-, 60-, or 90- days.

3.2.2 E-Mail Best Practices

Best practices need to be articulated in your organization's e-mail management policies or procedures. The following four sections provide guidance and suggestions that address saving messages, handling attachments, naming conventions, and applying retention and disposition schedules.

Saving E-mails

To facilitate the retrieval, retention, and disposition of messages, it is important to know if employees save messages to locations external to their e-mail clients. If these practices exist and they are permitted, you may want to incorporate into your e-mail policy or guidelines instructions for how and where employees should save messages. Recommendations may include:

- Deleting the original message from the e-mail client once a copy of the message has been saved to another location;
- Using naming conventions for saved e-mails;
- Not altering the contents of the message; this includes the subject line or the redaction of any information in the text body;
- Saving the message in a manner that ensures that all its original components are retained, including the message's header information, metadata, and any attachments that accompanied it; and
- Identifying the locations where e-mails may be saved.

Handling Attachments

As mentioned in Section 2.1.4, an authentic e-mail is one that contains its full text (including header information), any attachments, and all metadata associated with that message. Every attempt to should be made to maintain the bond between the original message and any attachment downloaded from it. How and where employees save and download e-mail attachments depends largely on your organization's e-mail technological capabilities.

One way to attempt to limit the dispersal of these documents may be to implement new policies or procedures for how employees manage their attachments. Policies specifically involving e-mail attachments may recommend staff to:

- Only download attachments that are vital for their duties.
- Preview, in the e-mail client, attachments that the recipient does not need to act upon (Figure 6). This feature may not be available for some e-mail clients. Previewing attachments minimizes wayward documents (i.e., documents saved to erroneous locations on the person's computer or the organization's shared network drive), thereby helping to curtail unnecessary digital duplication. **Warning:** Viewing an attachment does *not* prevent the spread of computer viruses. Never open an e-mail from an untrustworthy source.
- If the e-mail client does not have a preview feature, the attachment should be downloaded, viewed, and then deleted when it is no longer needed.
- Use file naming conventions for attachments that need to be downloaded and saved for later use or reference (see below for Naming Conventions)
- To reduce the number of attachments being sent between co-workers, if your organization uses an EDRMS or shared network drive for document management, provide links to the document(s) in the body of the message rather attaching the document(s) to the message. **Note:** This will only work if the persons receiving the message have access to the document's location.

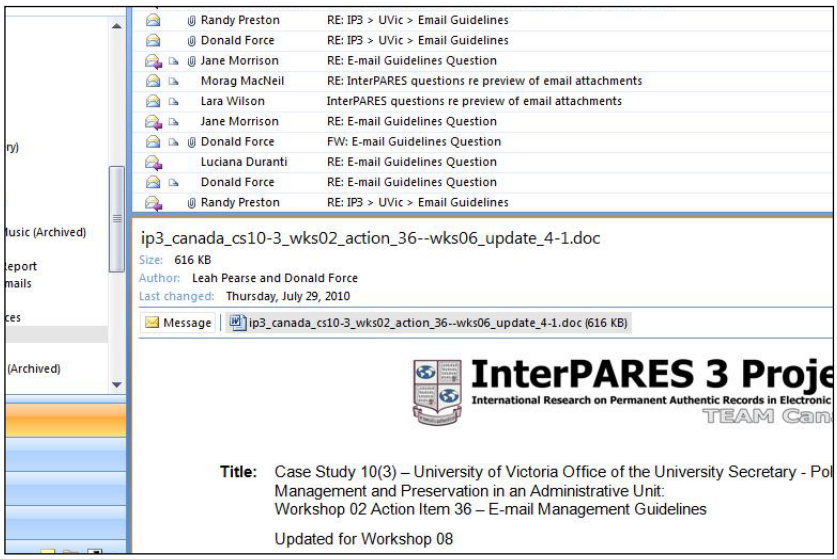

Figure 6: Previewing an Attachment (Microsoft Outlook)

Naming Conventions

When saving attachments, establishing a set of naming conventions for filenames may help maintain the connection between the downloaded document and the original e-mail. You should collaborate with all the relevant stakeholders to devise the most effective set of file naming conventions for your organization. Any naming conventions created for e-

mails should be made in conjunction with specific work processes and other documents that result from them. In other words, naming conventions should not be unique to the e-mail format. The following is a list of suggested fields you may want to include:

- **Date** – The date on which the e-mail with the original attachment was received. This should be indicated by using the international standard format of YYYYMMDD with no spaces or extra punctuation.
- **Subject** – This could be the attachment's original filename. If the filename lacks a clear description, once downloaded, it should be changed to better reflect the nature of the document. The subject given to the filename should be as concise as possible.
- **Type** – An abbreviation identifying the document's type. Abbreviations should be developed per each unit's needs and purposes, though some suggestions for abbreviations include:
  - AGD (Agenda)
  - AGR (Agreement)
  - BRN (Briefing Note)
  - CON (Contract)
  - DFT (Discussion Draft)
  - GRA (Grant)
  - IDX (Index)
  - LTR (Letter)
  - LST (List)
  - MEM (Memo)
  - MIN (Minutes)
  - MTG (Meeting)
  - NTS (Notes)
  - POL (Policy)
  - PRS (Presentation)
  - PRC (Procedure)
  - RPT (Report)
  - SPE (Speech)
- **Version Control Number** – This number tracks changes to a document and helps a user determine its currency and history (i.e., previous iterations and number of major changes).

Applying Retention and Disposition Schedules

Like all other types of organisational records, retention and disposition schedules need to be applied to e-mails. Like all other electronic documents, keeping every sent and received e-mail is simply not a sustainable long-term option. Ideally, e-mail should be treated the same as any other digital record; a process that may be facilitated with the use of an EDRMS which will tightly integrate the disposition of records. The retention and disposition of e-mails should be based on function not form; placing messages in a folder classification structure based on the organisation's retention and disposition schedules may facilitate this process. Destroying e-mails based on a time-oriented strategy, such as 30, 60, or 90 days, or simply allowing employees to delete messages without proper guidance or instructions may, in some jurisdictions, be legally unreasonable or result in the erroneous deletion of important messages.

If your current e-mail documentation does not contain a diagram or flowchart that provides a visual representation about how e-mail should be handled, you might want to consider adding a diagram similar to the one depicted in Figure 7. This flowchart presents one of the ways in which you may visually show employees in your organisation that e-mails should be retained and disposed according to function not form. The flowchart provides examples of the different types of e-mails and specifies their retention and disposition periods.

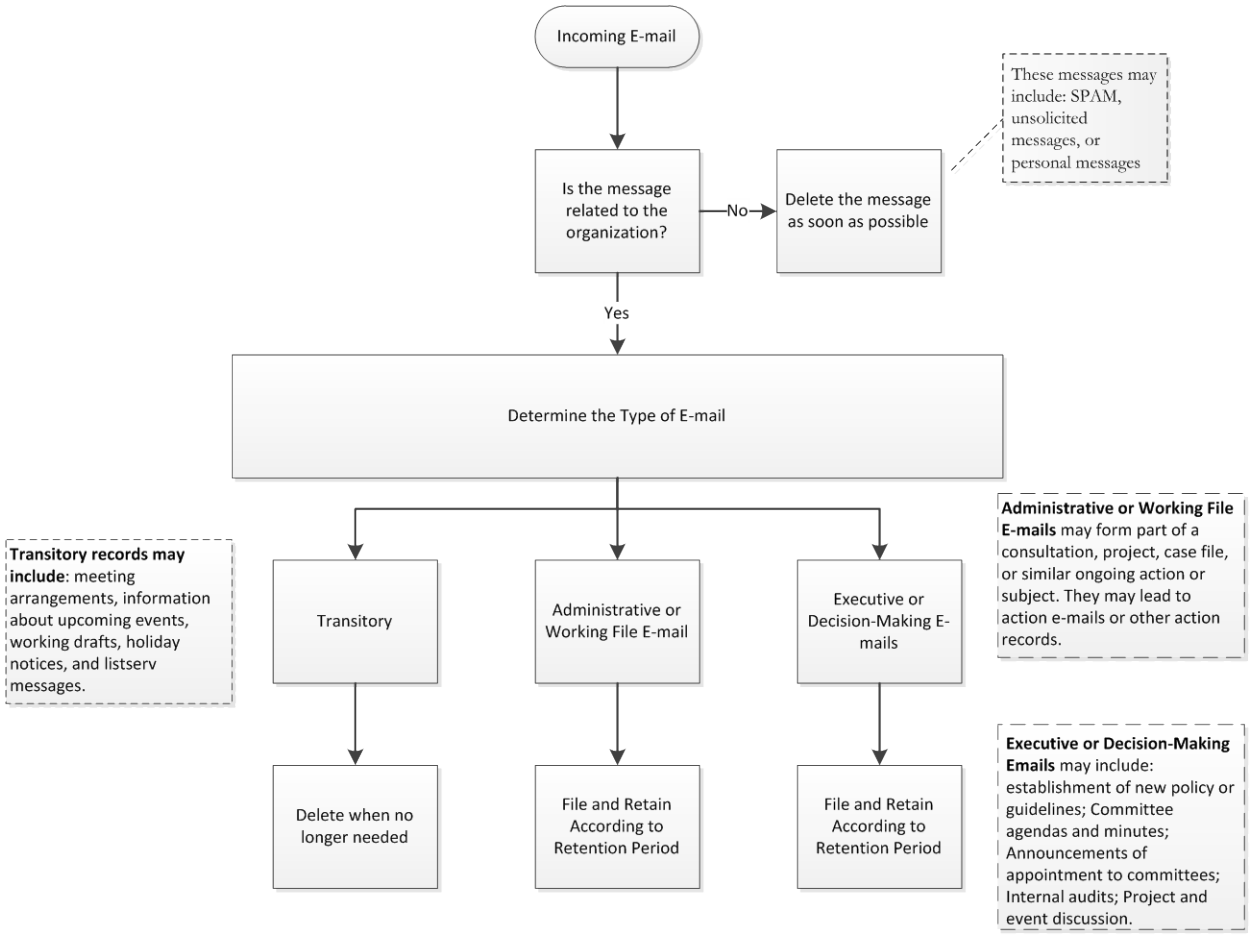

Figure 7: E-mail Management Flowchart

Exercises:

4. What may be the best method(s) for employees to manage their e-mail at your organisation?
5. What are some risks associated with saving e-mail and attachments to locations external to the e-mail client at your organisation?
6. As an employee of your organisation, do you destroy messages in accordance with the organisation's disposition schedules?

3.3 Determining Best Method(s) to Preserve E-mails

The long-term preservation of e-mail requires a substantial amount of resources. Not only does it require an in-depth skill set and knowledge of people familiar with e-mail's technological infrastructure, but it also requires a large amount of resources in terms of system design and capabilities to convert, normalize, store, and maintain messages. This is because e-mail preservation hinges on two primary issues: converting the message (and any attachments) into preservation and access formats and ensuring the retention of the message's significant properties. Of course, it is also necessary to have the proper tools when preserving e-mail.[4]

3.3.1 Conversion Formats

In situations where the organization relies on e-mail in a proprietary closed format, such as PST files, these should be converted and normalized to an open preservation format, the most popular of which include plain text, XML, or MBOX, which at the time of writing is one of the most common formats for preserving e-mails because it allows for one or more messages to be saved as a single file.[5] The purpose of converting e-mails to a different format is to allow the messages to be transferred into a digital repository system (DRS), such as Archivematic, DSpace, or Fedora. While an ECM/EDRMS is designed to facilitate the management an organisation's records from their creation through to their disposition, a DRS aims to provide the long-term preservation and access to records with permanent retention.

---

[4] A discussion of the tools that may be used to facilitate the preservation of e-mail goes beyond the scope of this module, suffice to say there are many programs and pieces of software available (free and for purchase). For example see Gareth Knight, "Significant Properties Testing Report: Electronic Mail," Investigating Significant Properties of Electronic Content (InSPECT) (March 2009). Available at: http://www.significantproperties.org.uk/email-testingreport.html (last accessed 5 January 2012) and Chris Prom, "The Power of Patience," Practical E-Records: Software and Tools for Archives (11 June 2010). Available at http://e-records.chrisprom.com/?p=1274 (last accessed 11 June 2011).

[5] For more information about MBOX see http://en.wikipedia.org/wiki/Mbox (last accessed 11 June 2011).

Plain text

Converting e-mails to text only is often known as converting the message to UTF-8 (UCS Transmission Format-8 bit), an extension of ASCII (American Standard Code for Information Interchange), "a character coding standard that has very few layout codes and no logical relationships."[6] Saving a message as text only presents a very basic rendition of the message, stripping it of any hyperlinks, images, attachments, and formatting (Figure 8).

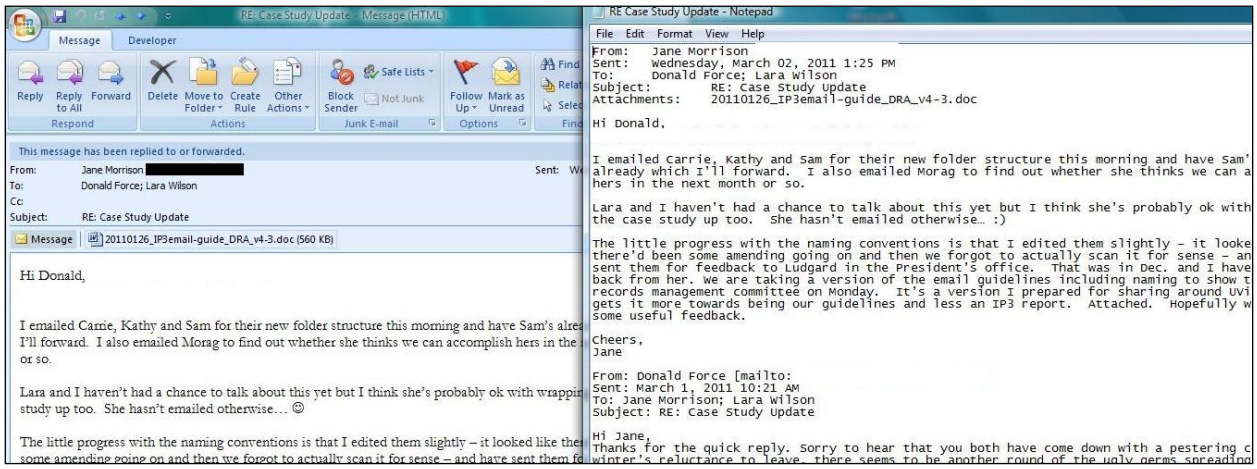

Figure 8: Text only (right) compared to the original Outlook message (left).

Some of the benefits of this format include retaining most of its basic formatting, such as the header information, message body, and signature. If the message needs to be preserved permanently, UTF-8 is based on an international standard (ISO 10646-1:2000) so the message may be accessible in future years and may be rendered using a variety of different programs such as Notepad, Wordpad, or an internet browser, such as Firefox or Internet Explorer.

Saving messages as text files does have several shortcomings. Any imbedded images or text written in different fonts (even something as simple as italics, bold, or underline) will be lost. Hyperlinks will no longer work, that is, if the link is imbedded in the text (e.g., InterPARES) its will become deactivated and the address will be lost. Moreover, saving messages as "text only" does not allow for attachments to be saved with the original e-mail; attachments must be saved as a separate process. Also, the message's metadata, the information about the message that is located in the Properties menu (see below) will be lost. With regards to a message's metadata, aside from the header information contained within the e-mail, all other metadata is lost. The "properties" menu of the text file applies only to the text file and not the original Outlook message. Finally, the text file is also writeable meaning the message's contents may be changed by a user accessing the file (the permissions may be changed).

---

[6] Charles M. Dollar and Thomas E. Weir, Jr., "Archival Administration, Records Management and Computer Data Exchange Standards: An Intersection of Practices," in *A Sourcebook on Standards Information: Education, Access, and Development*, Steven M. Spivak and Keith A. Winsell (eds.) (Boston: G.K. Hall & Co., 1991), 194.

XML

Converting messages to XML may be one of the surest ways to ensure the long-term preservation of e-mails. As one author explains, "XML representations are often used to prepare OAIS-compliant AIPs (Archival Information Packages), which wrap an e-mail, including all its components, together with its metadata, so that each e-mail is in a sense joined with the information intended to describe it."[7]

Converting e-mails to XML may be largely an IT operation, though there are a number of available tools (free and for purchase) that may be downloaded that extract e-mails from e-mail clients and convert them into XML format, such as PeDALS Email Extractor,[8] Aid4Mail,[9] and the Collaborative Electronic Records Project's E-mail Parser.[10] Without elaborate descriptive techniques, it may be less useful in those instances where a message has one or more attachments because the attachment(s) would have to be preserved separate from the XML document but linked via additional metadata within both documents (the converted e-mail and the attachment).

3.3.2 Significant Properties

Regardless of what format you ultimately decide to convert your e-mail messages to, you will need to keep in mind the core properties, or metadata elements, that need to be retained. The Investigating Significant Properties of Electronic Content (InSPECT) research project has identified 14 properties in the message header and 50 in the message body that "contributed information that established the authenticity and integrity of the email…."[11] These elements include, among others, ensuring the identification of the account name of the creator, sender, or recipient of the message; capturing the host of domain name; retaining the message body; and ensuring attachments maintain their relationship with the message. The InSPECT report emphasizes that the importance of the metadata properties will vary based on organisational and technological context; you must collaborate with your organisation's IT personnel to determine which fields best suit your organisation's needs.

3.4 Designing/Revising E-mail Management & Preservation Policy & Procedure(s)

---

[7] Massimiliano Grandi, "Guidelines and Recommendations for E-Mail Records Management and Long-Term Preservation," InterPARES 3 Project, TEAM Italy (v1.3, May 2010), 30-31. Public version forthcoming.
[8] PeDALS Email Extractor. Available at http://sourceforge.net/projects/pedalsemailextr/ (last accessed 30 May 2011).
[9] Aid4Mail. Available at http://www.aid4mail.com/ (last accessed 30 May 2011).
[10] Collaborative Electronic Records Project (CERP). Available at http://siarchives.si.edu/cerp/parserdownload.htm (last accessed 30 May 2011).
[11] Knight, "Significant Properties Testing Report: Electronic Mail." It is beyond the scope of this module to list and discuss all these elements. Please refer to this report for a complete listing of the recommended properties, their definitions, and additional information about their importance.

3.4.1 Management & Preservation Policies

Based on the information you accumulated in the previous steps, it is now time to design new (or revise) e-mail management and preservation policy(ies). Depending on the policy hierarchy of your organization, new documentation about e-mail management and preservation may be a standalone document or it may be part of a broader policy, such as your Information Technology's Information Use Policy. Overall, how you structure your policy will be based on your organization's contextual information.

In addition to the elements outlined in the Policy Module, e-mail management and preservation documentation should include the following sections:

Personal Messages, Security, and Privacy

This section may include the level of expectation of privacy the employee may have when using his/her e-mail client at his/her work station. The section may also address the extent to which an employee may or may not be allowed to use other e-mail systems, or send personal messages, during working hours.

Statement of Responsibility

Since an e-mail may be sent to multiple persons, it is important to identify who is responsible for the message, and thus, its retention. The Australian National Archives' "Guidelines on Developing a Policy for Managing Email" recommends that for messages sent internally and without attachments, the sender or initiator of an e-mail dialogue is the person responsible for saving the message.[12] The sender of the message is also responsible for any message that is sent outside the organization. If a message is sent from an outside source and received by more than one person within the organization, the person in the area of work relating to the message is the one responsible for the e-mail. The retention of messages with attachments and message exchanges between three or more people will be based on the organization's functions and work processes directly related to the subject of the correspondence.

E-mail Attachments

A document attached to an e-mail is usually an important component of that message. In many situations, attachments should be kept with or remain associated with any e-mail. This section of the policy should articulate how attachments should best be handled at the organization, such as reiterating the importance of not removing attachments from e-mails or downloading attachments and deleting the original message if the message contains relevant information about the attachment.

Saving E-mails

This section should articulate the organization's position toward the employee being able to save messages external to the e-mail client. If employees are allowed to save messages outside the e-mail client, the section should identify the location(s) or media to which e-mail may be saved.

---

[12] Eleanor Russell, "Guidelines on Developing a Policy for Managing Email," Surrey, Australia: National Archives (2004). Available online at http://www.nationalarchives.gov.uk/documents/information-management/managing_emails.pdf (last accessed 12 June 2011).

Retention and Disposition

This section should articulate the organization's position on the retention and disposition of e-mail. For example, the section should convey to the employee if the organization subscribes to a specific time-oriented retention period (e.g., 60 or 90 days) or if employees should apply established retention and disposition schedules to their messages. This section may also include how the organization handles an employee's e-mails when he/she no longer works for the institution.

3.4.2. Management & Preservation Procedures

As mentioned in the Policy Educational Module, procedures are prescriptive actions or operations which, when performed, result in a prescribed result or outcome. Procedures are the implementable actions that enable policy to be put into practice. Since this documentation will be based on the organization's technological resources and social infrastructures, each organization will have its own unique set of procedures for managing and preserving messages based on the information obtained in steps 2.1-2.3.

Procedures should be designed in close collaboration with relevant stakeholders. Soliciting feedback from employees and allowing them to contribute to the development of management and preservation policies, procedures, or guidelines, may reduce the amount of organizational cultural resistance that may occur when employees are requested to adjust the ways in which they manage their e-mail.

Exercises:

7. What format(s) do you foresee you organisation converting e-mails into for preservation? Why?
8. If your organisation already has an e-mail management or preservation policy, what sections or elements might you add or revise to the documentation?

3.5 Implementing E-mail Management & Preservation Policy(ies) & Procedure(s)

The final step in the EMPM is to implement the new policies and procedures that you have created. The documentation may be facilitated by educational seminars or workshops that introduce them and discuss how it is expected that they be complied with. As discussed in the Policy Module, these documents should be supported by senior management and all employees should be required to sign-off on them to acknowledge their willingness to comply with the new methods and procedures. The acceptance or final distribution of the e-mail management and preservation policies and procedures should not result in their finality. Every effort should be

made to revisit the policies and guidelines on a regular basis (e.g., twice a year for the first year of deployment and once a year thereafter) and update them as technologies change, the organization changes, and the surrounding environment to the organization changes.

4 Case Study: Development of E-mail Management Guidelines in an Administrative Unit at an Academic Institution

This section discusses an InterPARES 3 (IP3) case study that involved the development of e-mail management guidelines in an administrative unit at an academic institution. This case study offers an example of how the EMPM may be applied. The organization's name has been anonymized.

It should be noted at the outset, that the University acknowledged that it did not have the necessary resources (i.e., technological, staff, time commitments, etc.) to develop a strategy for the long-term preservation of its e-mail. The goal of this study was to gain better control over e-mail management within one particular office; this progress would facilitate any future efforts to preserve those messages identified as having long-term value to the office and the University. Moreover, the guidelines, rather than an e-mail management policy, were created because the case study targeted one specific University unit. As the guidelines are adopted by other units, it is expected that the documentation will form the base of a university-wide policy on e-mail management.

4.1 Background on Organization

Douglas University (DU – a fictitious name) joined InterPARES3 (IP3) as a test bed partner in order to devise e-mail guidelines for staff within the Office of Administrative Importance (OAI). Although e-mail is the primary means of conducting business activities at OAI, management of e-mail documents is unregulated and is left to the discretion of each employee.

The OAI at DU was established in 1955 and operates as the corporate secretariat to the governance bodies of the University and is responsible for University-wide elections, senior advisory committees and matters relating to Freedom of Information and Protection of Privacy Act compliance. The OAI consists of approximately 8 full-time staff members.

4.2 The Challenges

This case study faced two major challenges: 1) the Office of Administrative Importance did not use an electronic document and records management system (EDRMS) for managing its digital records and/or e-mails; and 2) e-mail management was unregulated and left to the discretion of each employee.

4.3 The Process of Guideline Development & Implementation

Step 1: Identify E-mail Context

In order to gather all the important information about the organization's records management principles, technological capabilities, organizational culture tendencies, and legal issues, the researchers working on the case study interviewed the university's records professionals and the select staff from the OAI (time restrictions prevented all staff from being interviewed). Some of the findings of this phase of research included:

Records Management Principles

- The University uses a classification and retention and disposition schedule for its records, what it calls, the Directory of Records (DOR). The scheme identifies 12 high-level functions of the University.
- Though employees are encouraged to use folders related to the formal ones designated by the DOR, many individual users maintain their own filing systems (often alphabetical and/or subject-based) both for paper and digital records.
- Additionally, it was learned that the University already had a "Guidelines for Managing E-Mail" document, but its content needed to be revised, updated, and presented in a more aesthetically pleasing way.

Technological Capabilities

- All UOI staff create and manage e-mails using PCs and Microsoft Outlook 2003, which is run on an Exchange server.
- Staff receive 500 MB of disk space on their Exchange Accounts.
- Backups of the e-mail server occur on a nightly basis and are performed by a division within the IT Department.

Legal Issues

- National or Regional binding legislation:
    - Freedom of Information and Protection of Privacy legislation
    - University Foundations Act
- University binding policies:
    - Responsible Use for Information Technology Services
    - Discrimination and Harassment Policy and Procedures
    - Policy Regarding Access to Student Records
    - Policy for Complaint Records

Organizational Culture Tendencies

- Interviewed staff within the OAI expressed a wiliness to receive guidance for better managing their e-mail; they acknowledged that this information would help them become more effective and efficient in their positions.
- Most interviewed staff already had some type of self-created folder classification structure in place for managing their e-mails, but with varying complexity and adherence (i.e., some staff had folders in place but simply lacked the time to regularly classify messages).
- Most staff felt quite comfortable with the way they handle e-mail attachments, but recognize that they manage them inconsistently; most expressed some desire to know how they should handle e-mail attachments.
- Retention and disposition of e-mail was typically done *ad hoc*.

Step 2: Determine the best way(s) to manage e-mail

Based on the findings in Step 1, several decisions were made regarding the content of the e-mail management guidelines:

- Staff needed information about how to determine if an e-mail should be retained or destroyed.
- Staff should be strongly encouraged to modify their folder classification structures in accordance with the University's DOR. This decision was based on the observation that all staff interviewed relied on some type of personalized folder structure to manage their e-mails and the records management office had no intentions of implementing a university-wide EDRMS.
- Staff needed guidance for how best to minimize the downloading of attachments.
- Staff needed guidance for how to name e-mails and/or attachments that they save outside the e-mail client.

Step 3: Designing E-mail Management Guidelines

While the University already had its "Guidelines for Managing E-Mail," it was decided to create an entirely new set of guidelines that incorporated the contextual information collected during Step 1 and decisions in Step 2. The guidelines would be as short as possible. Knowing the fast-paced environment of the OAI and the limited time that staff had to read and apply the documentation multiple documents involving e-mail management would not suffice (e.g., the guidelines as a standalone document, a procedural document on managing attachments, a document discussing naming conventions, etc.).

The designing of the e-mail management guidelines was not a process done only by the University's records professionals. Constant feedback was sought from OAI regarding drafts of the guidelines. The open communication about guidelines aimed to identify the language that pleased all parties but contained the essential records management content while being useable by the OAI (and other units to follow).

Overall, the guidelines stretched to six pages and the primary sections of the guidelines include:

- Privacy;
- Relevant legislation;
- Identification of which e-mails should be retained and which should be disposed of and when;
- Directory of records;
- Manage attachments; and
- Naming conventions.

See Section 4 of this module for the "E-mail Management Guidelines."

Step 4: Implement the E-mail Guidelines

The University's records professionals implemented the guidelines per the University's procedures. Each staff member of the OAI received a copy of the guidelines acknowledged that he/she would adhere to them. Since OAI staff worked with the University records professionals, there was a minimal amount of resistance to the implementation of the guidelines. In the months after the staff received the new guidelines, each staff member worked with the records professionals to match their inbox folder schemes to the DOR. The process identified the one weakness of the e-mail guidelines—convincing staff to delete messages according to the

disposition section of the document. The crosswalk procedure resulted in staff realizing that certain messages could be destroyed or they simply did not need other messages because they resulted from functions that had been designated. Yet, it would be impractical for the records professionals to regularly checkup on all University employees to verify they properly retain or destroy their messages. Aside from this matter, the guidelines helped clarify, among other issues, personal concerns about how to handle attachments and how to name any messages they save external to their e-mail client. Moreover, staff also feel more confident in their e-mail management practices knowing that each member of their office follows the same set of guidelines. The guidelines remain open to revision and the records professionals regularly seek feedback to improve their usability and effectiveness.

5 Templates

In addition to the following example, there are a wide range of e-mail management and preservation policies and guidelines available on the Interne. You must determine the format and use of language that is most appropriate for your organization.

E-mail Management Guidelines

Douglas University

Introduction

The use of e-mail at Douglas University (DU), like the creation and use of other records, is meant to support the University's teaching and administrative business. All e-mails created and received in support of this business are University records. Managing e-mail records therefore enables the University to meet its administrative needs, legal obligations and to retain its corporate memory. All records management activities are a legitimate part of daily work; making time to manage e-mails regularly can be more efficient overall and can actually assist in workload management. This document is designed to facilitate this process.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to all records in the custody or under the control of DU. The university is obligated to ensure that applicants receive any records to which they are entitled under the Act. If any university employee receives a Freedom of Information (FOI) request, that employee **MUST NOT** delete any e-mails responsive to that request. Contact the Associate Archivist, the University Privacy Officer, or the University Secretary's Office for further information about FOI requests.

Do not use non-DU e-mail accounts for university business. Confidential business information and personal information requiring privacy protection should not be maintained outside the university's information systems.

Under FIPPA, the university must store and access personal information in its custody or under its control only in Canada, unless the individual the information is about has consented to the particular instance of storage and access in another jurisdiction. Many webmail services operate on servers based in the U.S. and use of those services for e-mail containing personal information would contravene FIPPA.

Create e-mails and organize files with access in mind. Be objective and factual when writing about individuals.

Set up unit practices for managing confidential e-mails, including the following: have an explicit statement of confidentiality in policy, procedure or notice within the process that produces the e-mail; have a written request for confidentiality from the sender (in addition to the usual e-mail footer); send e-mail only to those persons permitted by procedure to have access to the confidential information. Be aware that certain provisions of FIPPA may take

precedence over confidentiality.

DU Records Management Policy

The university's Records Management policy and procedures provide direction on the creation, use and disposition of university records, access to the records, and define authorities, responsibilities and accountabilities for records management.

E-mail Security

Ensure smartphones and mobile computing devices are, at a minimum, password-protected in order to protect your e-mail account from unauthorized access.

Do not open unexpected attachments, and never respond to an email asking for personal account information.

Keeping E-mails

What to keep

You will need to keep many e-mail messages for certain lengths of time. The following checklist can aid in deciding which to keep.

- could the e-mail be used as evidence of an action or a decision about an individual, a program, project, etc.?
- does the e-mail contain information that will be used as a basis for future decisions?
- does the e-mail require or authorize an important course of action?
- does the e-mail approve formal policy or set a precedent?
- does the e-mail detail any obligations or responsibilities of the University?
- does the e-mail protect the rights or assets of the University or its stakeholders?
- is your unit primarily or jointly responsible for maintaining the original, authoritative record about the individual, program, project, etc.?

If the answer to any of these questions is 'yes,' the e-mail and its attachments should be kept for its appropriate retention period. These messages are considered Action E-Mails.

If the answer to all of these questions is 'no,' then the e-mail should be deleted either when it is no longer useful, if it is transitory, or when its retention period is finished, if it is part of a working file.

Further examples of Action E-mails include: discussions and recommendations relating to programs, students, personnel and policies that are not of a routine nature; substantial information about the unit, its personnel, students or programs; and/or actions, decisions or commitments of the unit. Many messages related to projects, activities, or certain subjects may have a specific retention period; please consult the Directory of Records (DOR) for this

information (see Organization section for more details).

Administrative / Working File E-mails

Many e-mails will be neither action nor transitory messages. These can be thought of as part of "working files" and are e-mails that form part of a consultation, project, case file, or similar ongoing action or subject. They may lead to action e-mails or other action records.

These messages should be filed with action e-mails in the appropriate e-mail folder. If time permits, manage them by deletion when they are no longer needed to document an action or a decision; otherwise, apply the appropriate records retention period to the entire e-mail folder. See the sections below on organization and disposition.

Transitory E-mails

These are only required for a limited period of time for the completion of an action, the preparation of an ongoing record, or are purely for informational purposes.

Transitory records may include: meeting arrangements, information about upcoming events, working drafts, holiday notices, and listserv messages.

Organization and Storage

E-mail cannot be classified or disposed of purely based on its format as an electronic message. Furthermore, MS Outlook is not designed to meet international records management standards and therefore is not suitable to be used for long-term storage of e-mail records.

Using folders based on function, subject, activity or project often makes for more effective management of e-mail. These types of organization facilitate searching and retrieval; they also enable simple disposition by applying retention/ disposition rules to entire folders.

DU's records classification and retention plan, the DOR, provides rules on how long to keep records and information and when to dispose of them. At a minimum, you can use the DOR to organize your top-level folders. The DOR arranges all University records by functional categories and supplies retention periods for them (if the retention period is blank, contact the Associate Archivist for guidance).

The 12 functional categories in DOR are:

Administration	Buildings and Properties
Computing and Systems Services	Financial Management
Governance	Human Resources
Libraries, Archives and Museum	Research
Safety and Security	Student Records

Student Services Teaching Programs

Organizing by functional category, activity, or project is recommended over using only the inbox and sent folders. In this way, action and administrative/working file e-mails can be maintained in Outlook (for their retention period) while keeping the inbox and sent folder contents at a minimum.

E-Mail Attachments

A document attached to an e-mail is usually a vital component of that e-mail. It is important that attachments are kept with or remain associated with any e-mail that is of long-term importance. This guideline is designed to help users better control where they save and access downloaded attachments while minimizing duplication and reducing version control mistakes.

- Never delete an attachment from its original e-mail.
- Only download the attachment and delete the original e-mail if:
    - the attachment is needed *and*
    - the accompanying e-mail does **not** contain information about the attachment *and*
    - the message is transitory (see above).
- Preview attachments if:
    - you only want the document for reference purposes
    - you do not need to take action on the document (i.e., revise or edit).

    Note: Viewing an attachment does **not** reduce the risk of receiving a virus! Never click on an attachment that accompanies an e-mail from an unknown sender!

Previewing Attachments

- To view an attachment and your reading pane is **on**…
    - Single left-click the attachment. A preview of the document will appear in the reading pane (Figure 4).
    - You may be asked to verify the trustworthiness of the attachment before viewing (Figure 5).
    - Never preview an attachment from an unreliable sender.
    - Not all file types may be previewed; in these circumstances, if the attachment is trusted, it should be downloaded according to the procedures outlined below.

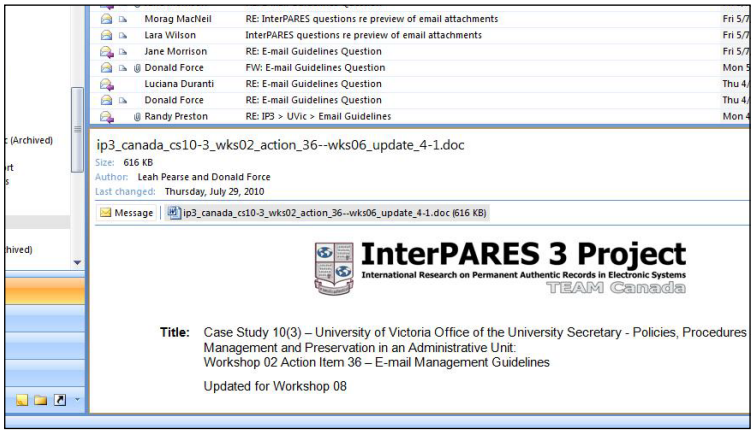

Figure 9: Attachment being Previewed

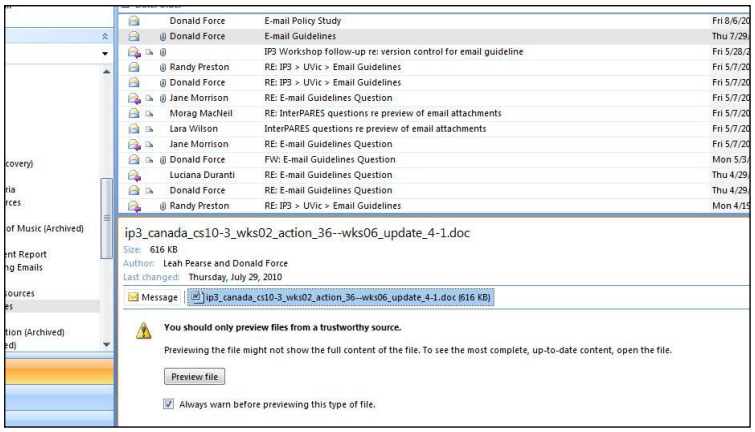

Figure 10: Verification to Preview Attachment

- To view an attachment and your reading pane is **off**…
    - Double-click the e-mail to open it in a new window.
    - Single left-click the attachment. A preview of the document will appear in the reading pane (Figure 4).
    - You may be asked to verify the trustworthiness of the attachment before viewing (Figure 5).
    - **Never** preview an attachment from an unreliable sender.
    - Not all file types may be previewed; in these circumstances, if the attachment is trusted, it should be downloaded according to the procedures outlined below.

Downloading Attachments

If an attachment needs to be downloaded for revision or reference, the following steps should be taken:

- If the reading pane is **on**:
    - Double-click the attachment;
    - Select "Open";
    - "Save As…" the document to the appropriate location and with an appropriate filename (see below for filename conventions).
- If the reading pane is **off**:
    - Double-click the message to open it in a new window;
    - Double-click the attachment;
    - Select "Open";
    - "Save As…" the document to the appropriate location and with an appropriate filename (see below for filename conventions).

Document Naming Conventions

Once an attachment is downloaded from the original message, its filename may need to be changed, especially in those situations where the original filename lacks a useful description. Editing this filename may be a way to maintain the connection between the downloaded attachment and the original e-mail. This section offers suggestions for consistently naming filenames.

It is important to ensure that a downloaded attachment maintains a relationship to its original e-mail message. To sustain this link, the filename of the downloaded attachment should contain certain information.

Date

The date should be the date on which the e-mail with the original attachment was received. This should be indicated by using the standard format of YYYYMMDD with no spaces or extra punctuation.

For example, if you received an e-mail with an attachment that you downloaded on January 5, 2010, the date would be represented as 20100105.

Subject

This could be the attachment's original filename. If the filename is not that descriptive, once downloaded, it should be changed to better reflect the nature of the document. The subject

given to the filename should be as concise as possible.

For example, if you received these guidelines as an attachment and downloaded them, instead of naming it University_of_Victoria_E-mail_Guidelines, the subject could be EmailGuide.

Type

Following the subject, the document's type should be identified. This should be listed as an abbreviation. Units are encouraged to develop a document type list for their purposes. Suggested abbreviations include:

AGD (Agenda)	AGR (Agreement)	ARS (Action Request)	BRN (Briefing Note)
CPA (Cover Page)	CON (Contract)	DFT (Discussion Draft)	EXA (Example)
FRM (Form)	GRA (Grant)	IDX (Index)	LTR (Letter)
LST (List)	MEM (Memo)	MIN (Minutes)	MTG (Meeting)
NTS (Notes)	PLN (Plan)	POL (Policy)	PRS (Presentation)
PRC (Procedure)	RPT (Report)	SCH (Schedule)	SPE (Speech)
SUM (Summary)	SUP (Supplement)		

For example, if you received these guidelines as an attachment and downloaded them, instead of naming it University_of_Victoria_E-mail_Guidelines_Procedures, the subject could be EmailGuide_PRC.

Version Control

Version control tracks changes to a document and it helps a user determine its currency and history (i.e., previous iterations and number of major changes). The version number consists of the letter 'v' (representing the word "version") and two numbers separated by a dash (e.g., v2-1). The first number represents major changes, such as changes of decision, reorganization of content or presentation. The second number represents minor changes, such as corrections of typos, stylistic changes, minor additions or deletions.

In this example, the different components are as follows:

- 20100210 (date the e-mail with the attachment was received)
- EmailGuide (subject of the document)
- PRC (type of document; in this case, it is a procedure)

- v1-1 (the first minor modification of the first major version)

Contacts

Archives and Records Management staff are available to assist you. We are located in Douglas Library/Mearns Centre. We are happy to visit your office to discuss records management.

Bob Smith, University Archivist

(123 456-)7890 / bobsmith@du.edu

Jane Doe, Associate Archivist (Records Management and Access)

(123 456-)7890 / janedoe@du.edu

Related DU Policies, Procedures and Guidelines

In addition to these guidelines, please also refer to the following:

- Policy IM7700: Records Management Policy
    - Includes the Procedures for the Management of University Records and Procedures for Access to and Correction of Information
- Policy IM7200: Responsible Use for Information Technology Services:
- Policy GV0235: Protection of Privacy Policy:
- The Directory of Records (DOR)

6 Review Questions

- What are the four phases of the E-mail Management and Preservation Model (EMPM)?
- What are the four different types of contextual information that should be gathered during the initial phase of the EMPM?
- What are some of the legal ramifications that may result from poor e-mail management?
- E-mails should be retained and disposed according to their format or function? Explain.
- Identify at least three important components of any e-mail policy. Discuss each of their contributions to an e-mail policy.
- What is/are the best way(s) for managing e-mail (e.g., no classification, classification scheme, filing system, EDRMS, etc.)? Explain.
- What are the two primary requirements necessary for preserving e-mail?
- What are the three generally accepted formats when converting e-mail from its native format for its long-term preservation?

7 Additional Resources

The following list is not, nor is it intended to be exhaustive, but is intended to offer a selection of available resources for developing documentation for maintaining and preserving e-mail. They are chosen because they are seminal works in the field, offer the results of influential original research, and reflect collective "best-practice" knowledge from a particular area of discipline or community of practice. Many of the sources listed here also include bibliographies that will lead the reader to a broader network of resources.

Author(s) / Editor(s): ARMA International
Title: Requirements for Managing Electronic Messages as Records (ANSI/ARMA 9-2004)
Publication Date: 2004
Source/Publisher: ARMA International

Approved by the American National Standards Institute (ANSI), this standard "define[s] the requirements for developing a corporate policy for managing information content in electronic messages." From developing a policy team to ensuring that a disaster recovery plan is in place, this standard outlines the requirements necessary for implementing e-mail policy. Sections 7-9 focus specifically on the components that an e-mail policy should contain, such as addressing security, user compliance, encryption, content, attachments, and retention and disposition. This standard, though light on content, is a good starting point for a records professional wanting to implement an e-mail policy within his/her organization.

Author(s) / Editor(s): Artefactual Systems
Title: Archivematica: Open Archival Information System Wiki
Publication Date: 2011
Source/Publisher: Artefactual Systems
URL: http://archivematica.org/wiki/

Archivematica is a comprehensive digital preservation system that is free for public download and comment. This wiki contains information about the system and its developments as well as some information specific to the normalization of files to preservation and access formats (see Media type preservation plans link on main page).

Author(s) / Editor(s): Canadian General Standards Board
Title: Electronic Records as Documentary Evidence (CAN/CGSB-72.34-2005)
Publication Date: 2005
Source/Publisher: Canadian General Standards Board

This standard does not specifically focus on e-mail management or preservation, but it provides guidance for managing nearly all types of electronic records. The standard provides guidance on the management, storage, and preservation of electronic records to enhance their admissibility in a court of law. The standard focuses on the importance of establishing reliable recordkeeping systems by addressing the retention and disposition of records, ensuring their accessibility, implementing important security measures, and conducting audit and quality assurance processes.

Author(s) / Editor(s): Boudrez, Filip and Sofie Van den Eynde
Title: E-mail Archiving
Publication Date: 2002
Source/Publisher: DAVID Research Project
URL: http://www.expertisecentrumdavid.be/davidproject/teksten/Rapporten/Report4.pdf

While this report may be on the cusp of being dated, most of its findings still stand with regards to e-mail preservation. This report produced from the Flemish Digital Archiving in Vlaamse Instellingen en Diesten (DAVID) research project, discusses the benefits and drawbacks of several e-mail archiving and preservation tactics, such as retaining e-mail via the mail server or external to it by converting it to another format such as eXtensible Markup Language (XML), Hypertext Markup Language (HTML), or even as a Portable Document Framework (PDF). The project advocates converting messages to XML. In addition to its discussion regarding e-mail preservation, the report also addresses other issues associated with e-mail, namely, e-mail privacy and legislation as it pertains to Europe in 2002.

Author(s) / Editor(s): Knight, Gareth
Title: Significant Properties Testing Report: Electronic Mail
Publication Date: March 2009
Source/Publisher: Investigating Significant Properties of Electronic Content (InSPECT)
URL: http://www.significantproperties.org.uk/email-testingreport.html

"This report examines the notion of significant properties as it applies to electronic mail, a common form of digital communication. It seeks to identify the significant properties of email that must be maintained by examining each of its constituent elements and analyzing their designated function. It goes on to examine strategies that may be utilized to maintain access to e-mail assets in the long-term. Finally, it outlines a set of experiments that were performed by the project team to identify and evaluate tools that may be utilized to convert significant properties from one form to another" (author's abstract). The project was funded by the Joint Information Systems Committee (JISC).

Author(s) / Editor(s): Loughborough University
Title: Institutional Records Management and E-mail
Publication Date: 2003
Source/Publisher: Loughborough University, UK
URL:
http://www.webarchive.org.uk/wayback/archive/20070302174042/http://www.lboro.ac.uk/computing/irm/index.html

This was a six-month project funded by the Joint Information Systems Committee (JISC) where Loughborough University conducted six cases that investigated the management of e-mail as institutional records. As part of the research, the project interviewed e-mails users from different units within the university and designed an e-mail policy or guideline template that articulate the importance of policy statements and creating a diagram that depicts when messages should or should not be saved.

Author(s) / Editor(s): Mason, Stephen
Title: Archiving and Storing E-mails: The Legal and Practical Issues
Publication Date: 2007
Pages: 176-180
Source/Publisher: Computer Law & Security Report

"This article will outline the problems faced by one company in relation to the destruction of e-mail communications in a recent case in the United States, and then set out some of the legal and practical issues that lawyers and their clients should consider if they have reached the conclusion that they ought to buy one of the products that began to appear on the market from 2000 that help with the storage of e-mails in particular, although the issue is wider than just e-mail communications" (article's abstract).

Author(s) / Editor(s): Pennock, Maureen
Title: Managing and Preserving E-mails
Publication Date: 2006
Source/Publisher: Digital Curation Centre, UKOLN
URL: http://www.ukoln.ac.uk/ukoln/staff/m.pennock/publications/docs/RMS-b_mngmt-pres-emails.pdf

This article is the summarization of the author's larger report on a project she undertook to better understand the management and preservation of e-mails.[13] In this abridged version, she discusses legal issues (from a UK perspective), the different roles and responsibilities for creators and curators, and reviews how e-mails may be stored and preserved as authentic messages. Pennock argues that the long-term preservation of e-mail requires the messages to be converted from their original format into a more suitable format such as XML.

Author(s) / Editor(s): Prom, Chris
Title: Preserving E-mail
Publication Date: 2011
Source/Publisher: DPC Technology Watch Report 11-01, Digital Preservation Coalition
URL: http://www.dpconline.org/component/docman/doc_download/739-dpctw11-01pdf

Author(s) / Editor(s): Russell, Eleanor
Title: Guidelines on Developing a Policy for Managing Email
Publication Date: 2004
Source/Publisher: Australia: National Archives
URL: http://www.nationalarchives.gov.uk/documents/information-management/managing_emails.pdf

This document focuses on the key components that organizational e-mail management policies should address and what records professionals need to consider when managing e-mails as

---

[13] See Maureen Pennock, "Curating E-Mails: A Life-Cycle Approach to the Management and Preservation of E-mail Messages," DCC Digital Curation Manual (July, 2006). Available online at: http://eprints.erpanet.org/113/01/curating-e-mails.pdf (last accessed 5 June 2011).

records. The document provides examples for how the recommended sections may be worded. The author does not explore the technical underpinnings of e-mail or e-mail preservation.

Author(s) / Editor(s): Sedona Conference®, Working Group 1, Thomas Y. Allman (ed.)
Title: Commentary on Email Management: Guidelines for the Selection of Retention Policy
Publication Date: 2007
Source/Publisher: Sedona Conference
URL: http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110

Sedona Conference® is a nonprofit legal think tank consisting of lawyers, judges, academics, and other professionals based in the United States designed to address current legal issues and provide guidance to judges, lawyers, and other professionals to be able to move the law forward. This commentary focuses on the factors that readers should consider when designing or applying e-mail to retention and disposition policies; it also reviews the strengthens and weaknesses of different types of e-mail retention strategies with regards to their legal implications.

Author(s) / Editor(s): Wilkins, Jesse
Title: Technologies for Managing E-mail
Publication Date: 2008
Pages: 1-12
Source/Publisher: ARMA International
URL: http://www.arma.org/pdf/hottopic/feb2008.pdf

This article discusses the necessary components for an "e-message" management program. The author focuses on legal issues, from a United States perspective, involving e-mail management. The author emphasizes the challenges that e-mail poses during litigation, especially during the electronic discovery/disclosure (e-discovery), phase of litigation, where a party may be required to produce thousands, if not hundreds of thousands (or more) of relevant messages—without a reliable and effective system in place, retrieval and production of these e-mails will be a costly endeavor to the organization.

Appendix A: Contextual Information Worksheet

E-Mail Assessment Worksheet

Department / Unit Assessed:	
Assessor:	Date of Assessment:
Technological Context	
Type(s) of e-mail client	
Type(s) of server	
Space allocation (per inbox)	
System Backup Information (frequency of backups)	
Computer system(s) being used	PC ☐ **Notes:** Apple ☐ Other ☐
Information/records management systems being used	EDRMS ☐ **Notes:** Shared Network Drive ☐ Local Area Network ☐ Other ☐
Legal Context	
Federal/National Laws	
Provincial/State Laws	

Regional/Local Laws	
Case Law	

Organizational Context	
Policies	
Procedures	
Current E-mail Management Practices	No Classification ☐ **Notes:** Classification Structure ☐ EDRMS ☐
Attachment Management Techniques	
Saving E-mails Techniques	

Additional Notes:

Appendix B: E-Mail Attachment Questionnaire

E-Mail Attachment Questionnaire

Employee Name:

Department/Unit:

Date Completed:

This questionnaire defines "downloading" as the conscious process of saving an attachment to a specific location.

1) Do you perceive e-mails with attachments any differently than e-mails without attachments? Do you give them any more importance/value?

2) How do you download attachments?

3) Where do you typically download attachments to?

4) If you download an attachment and save it to your desktop/area network, do you rename the attachment?

5) How do you know which e-mail an attachment belongs to?

6) If you download an attachment and save it to your desktop/area network, do you download its accompanying e-mail and keep the two together?

7) If you print an attachment, do you print its accompanying e-mail? Visa versa?

8) Say you downloaded an attachment and made no edits to it. After a period of time, you need to refer to that attachment. Where do you go to access the document, your e-mail application or where you saved it?

9) Do you ever delete an attachment from the original e-mail? If yes, why?

10) Do you ever download both the e-mail and the attachment to keep them together? If yes, what format do you save the e-mail and attachments in?