National Electronic Commerce Coordinating Council

Managing E-Mail

Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

In 1997, as the use of the Internet was increasing at a stunning rate, a group of public and private professionals—government executives and information technology practitioners—met in San Antonio, Texas to discuss their common issues, problems and ideas. This first meeting was productive. Participants learned from each other. They felt that continuing to meet as a group would help them meet the challenges and opportunities posed by the rush of engulfing information technologies. This founding group formed the National Electronic Commerce Coordinating Council (NECCC), which has continued to meet regularly.

Today, NECCC serves as an alliance of government organizations dedicated to promoting electronic government through the exploration of emerging issues and best practices. Alliance partners are the National Association of State Auditors, Comptrollers and Treasurers; the National Association of Secretaries of State NASS; and the National Institute of Governmental Purchasing.

NECCC also works in partnership with these affiliate organizations: the Information Technology Association of America; National Automated Clearing House Association; National Association of Government Archives and Records Administrators; and National Association of State Treasurers

ACKNOWLEDGEMENTS

Charles Arp
John Aveni
Alvin Borromeo
Linda Hamel – Co-Chair
Robert Horton
Jerry Johnson
Alan Kowlowitz
Mark LaVigne
Roselyn Marcus
Drew Mashburn
Richard Pearce Moses
Martha Richardson
Dino Tsiboursi
Albin Wagner
Amelia Winstead – Co-Chair

CONTACT INFORMATION

The National Electronic Commerce Coordinating Council
2401 Regency Road, Suite 302
Lexington, KY 40503
P: (859) 276-1147
F: (859) 278-0507
www.ec3.org

2002 NECCC EXECUTIVE BOARD

SIGNATORY MEMBERS

Chair, *J. Kenneth Blackwell*, NASS, Secretary of State, Ohio
Vice Chair, *Ralph Campbell, Jr.*, NASACT, State Auditor, North Carolina
Secretary/Treasurer, *Mary Kiffmeyer*, NASS, Secretary of State, Minnesota

Steve Adams, NASACT, State Treasurer, Tennessee
David Dise, NIGP, Procurement Manager, Fairfax County Water Authority, Virginia
Rick Grimm, NIGP, NIGP Chief Executive Officer, Virginia
Stephen Gordon, NIGP, Purchasing Agent, Metropolitan Govt. of Nashville/Davidson County, Tennessee
Elaine Marshall, NASS, Secretary of State, North Carolina
Robert Childree, NASACT, State Comptroller, Alabama

AFFILIATE MEMBERS

P.K. Agarwal, ITAA, CIO and Executive Vice President, National Information Consortium
William Kilmartin, NACHA, Vice President, Accenture
Jack Markell, NAST, State Treasurer, Delaware
Amelia Winstead, NAGARA, State and Local Government Services Manager, Office of the Secretary of State, Georgia

EX-OFFICIO MEMBERS

Carolyn Purcell, CIO, Department of Information Resources, Texas
Basil Nikas, CEO, iNetPurchasing
J.D. Williams, Director, State and Local Government, PeopleSoft, USA, Inc.

AT-LARGE MEMBERS

Avi Duvdevani, CIO/Deputy General Manager, New York
Daniel Greenwood, Director, MIT E-Commerce Architecture Program, Massachusetts Institute of Technology
David Lewis, Retired Director and CIO, Massachusetts
Jay Maxwell, Senior Vice President, AAMVA
Eric Reeves, State Senator, North Carolina
David Temoshok, PKI Program Manager, Government Services Administration
Costis Toregas, CEO, Public Technology, Inc.
Susan Hogg, Chief, Statewide e-Government Initiatives Office

This page left blank intentionally.

TABLE OF CONTENTS

This page left blank intentionally.

MANAGING E-MAIL

EXECUTIVE SUMMARY AND INTRODUCTION

E-mail, like all new information technology, has been both a blessing and a curse for state government. On the one hand, it facilitates swift, accurate, paperless communication – a necessity in a civil society in which citizens expect the same efficiencies from government as they do from private sector businesses. On the other hand, e-mail use by government employees has opened a Pandora's box of problems: careless deletion of important government records that should be saved for practical or historic purposes; the dismay of employees who mistakenly thought their state-owned e-mail system could be used for embarrassing personal communication; unnecessary storage of thousands of e-mails that are the electronic equivalent of pink telephone message slips, resulting in burgeoning electronic storage costs; and the accidental transmission of e-mail to parties who were never intended to receive them, caused by the slip of a finger on a keyboard, to name but a few. As always, the successful introduction of new information technology in the workplace requires not only proper implementation of hardware and software, but adherence to a new roadmap of user behavior.

Some agencies have implemented fixed retention periods for e-mail to minimize the impact on the system. E-mail may be kept for as short as a month, often no more than three months. A single retention period for all e-mail means that many important messages may be destroyed, often before a legally required retention period.

Managing e-mail is particularly challenging because many underlying problems are technological. E-mail systems lack the necessary recordkeeping functions to properly classify, preserve, and dispose of messages. However, an equally important problem is human behavior. Without training and clear expectations, users cannot be expected to manage their messages well. Because e-mail is distributed on PCs throughout the organization – and in some instances, outside the organization – it is impractical to create centralized controls to support effective management. Ultimately, agencies must rely on users to manage their own e-mail.

Unfortunately, few employees have ever been taught how to use or manage e-mail. Similarly, managers cannot teach their employees best practices because those practices have never been clearly articulated. This document offers agencies models that can be adapted to establish policies and procedures for effective e-mail use and management.

This document is divided into three chapters: a model e-mail use policy, a model retention schedule and a model user's manual. The chapters are written for e-mail users, rather than administrators who are developing policies for implementation. Portions of the document that require implementers to make revisions based on agency-specific policy or procedures are flagged in the text in ALL CAPS or in footnotes.

SUMMARY: MODEL USE POLICY

This chapter offers a sample policy for state agency e-mail users. Its purpose is to establish acceptable behavior for proper business use of e-mail. It asserts

transmission of copyrighted materials, using e-mail to provide access to confidential material, inadvertent dissemination of e-mail, and e-mail ownership. It requires users to follow agency records management rules with respect to e-mails, forbids use of encryption unless authorized by the employee's supervisor and IT department, addresses anti-virus protection, and provides a central contact to answer users' questions about e-mail use and management.

SUMMARY: MODEL RETENTION SCHEDULE

States have different records retention laws, regulations and practices. This document, intended for use by state archivists and agencies developing retention schedules for state documents, suggests that all e-mail be categorized based on its value as a transient, reference, programmatic, administrative or policy/program development record (all defined in the model schedule).

The retention policy is grounded in the principle that e-mail, like any other record, should be filed and retained on the basis of its content. However, the schedule takes the pragmatic view that the content of most e-mail messages has only transient value. Hence, the policy emphasizes that it is not only acceptable, but also desirable, to discard those valueless e-mails immediately. The retention schedule attempts to clarify which e-mail messages are valuable to the agency, rather than letting employees assume that all messages should be kept because they might be valuable.

The schedule proposes three retention periods (immediate destruction, limited retention, and archival retention) for the sake of simplicity over efficiency. A three-year retention is certainly too long for many non-transitory, non-archival records, but avoids the need for a more complex classification system by preserving all records for the maximum retention period. Similarly, the schedule may preserve some records permanently that are of questionable value, rather than try to get users to learn subtle nuances of appraisal. Any retention period listed on schedules established by your state or agency will supersede the periods suggested here.

SUMMARY: MODEL USER MANUAL

This chapter describes the challenges associated with state agency e-mail use and provides guidelines for appropriate use: (e.g., accurately identifying the sender and recipient, creating a meaningful address line, including the original message when responding to an e-mail, and respecting privacy and confidentiality). It also discusses the limits on personal use of state agency e-mail, provides practical information about records management, and addresses the unique issues pertaining to viruses, encryption and security raised by e-mail use.

IMPLEMENTING THE MODELS

The wide range of social, business and technical environments makes it impossible for the models to cover all situations. When adapting these models for their own agency, administrators must consider the employees and customers who use e-mail, the potential risks associated with the business conducted via e-mail, the e-mail system, and the exact procedures employees should follow when using e-mail. For example, a legal or financial office may need to be more cautious about deleting e-mail than an office answering routine requests for information. Or, an agency that has many employees working offsite

using different e-mail systems will have to rely more on policies and procedures than an agency that has a centralized e-mail server.

More importantly, these models are only a beginning. Management must make it clear to employees that the agency has established standards for use and management of e-mail. Supervisors must see that employees receive adequate training in the agency's standards. Employees must be held accountable for complying with those standards.

Finally, because of rapid changes in e-mail systems, administrators must ensure that their policies remain current. In particular, agencies must address on-line messaging services, such as AOL Instant Messenger. To the extent that these services create no record, the messages are closer to a phone call. However, some messaging systems create records of the on-line conversations, and those records must be managed like e-mail.

SUMMARY

States can tailor these three chapters to their own organizations and legal environment to create e-mail policies, records management schedules, and user manuals that provide clear and consistent advice to their employee e-mail users.

This page left blank intentionally.

MODEL E-MAIL USE POLICY

TABLE OF CONTENTS

SECTION 1 - SCOPE

This policy applies to any e-mail message that is created or received by individuals using the AGENCY'S electronic mail (e-mail) service or that is created or received by employees in their official capacity using another e-mail system.

The AGENCY reserves the right to amend this policy at its discretion. In case of amendments, users will be informed of the change and the date the change is effective.

This policy does not grant users any contractual rights.

SECTION 2 – PURPOSE

This policy describes e-mail users' responsibilities for the proper use of the AGENCY'S e-mail service. The policy

- Ensures users are aware of what the AGENCY deems to be acceptable and unacceptable use of e-mail.

- Informs users that by use of the AGENCY's e-mail service the user agrees to comply with this policy and waives any right of privacy in any e-mail they create, send, receive or store in the system.[1]

- Places users on notice that the AGENCY can and may monitor use of e-mail without prior notification, and that the AGENCY reserves the right to take disciplinary action, including termination or legal action, if there is evidence that a user is not adhering to this policy.

SECTION 3 – RECORDS MANAGEMENT AND E-MAIL RETENTION

E-mail is a means of transmission of messages or information. The retention or disposition of e-mail messages is based on the information they contain or the purpose they serve. Because the content of e-mail or online messages may vary considerably, no single retention period applies to all e-mail messages.

[1] *Implementers: If the user signs an explicit acknowledgement to comply with this policy in Section 6, modify this section to read, "Informs users that use of the AGENCY's e-mail system waives any right of privacy . . . ."*

Therefore, message content must be evaluated to determine the length of time the e-mail must be retained. For information on scheduling and retaining e-mail messages, see RECORDS MANAGEMENT AUTHORITY.[2]

The content, transactional information, and any attachments associated with the e-mail are considered records, if they meet the criteria of STATE LAW.[3]

SECTION 4 - REQUIREMENTS

E-mail is a business communication tool, and users are obliged to use it in a responsible, effective and lawful manner. Although by nature e-mail may seem to be less formal than other written communication, the same laws apply.

The following rules are hereby created by the AGENCY and are to be strictly adhered to:

- The AGENCY'S e-mail service is intended to be used primarily for business purposes. Uses that interfere with normal business activities are strictly forbidden.

- E-mail use is subject to limitations as imposed by supervisors to prevent excessive or improper use. Although e-mail is meant for business use, AGENCY allows personal use if it is reasonable and does not interfere with work. However, the sending of chain letters, junk mail, jokes and executables is prohibited.

- Users shall not use e-mail for any for-profit business activities, operating a business for personal gain, sending chain letters, or soliciting money for religious or political causes. E-mail *may* be used to solicit money for charitable campaigns authorized by the AGENCY.

- Users shall not use e-mail for solicitation or to transmit or request material that could potentially embarrass the AGENCY. In particular, users are forbidden to download or transmit e-mails that are offensive, obscene, pornographic, threatening, or racially or sexually harassing. Receipt of unsolicited e-mail containing such material should be reported immediately to SUPERVISOR.

- Users shall not use e-mail to send or receive commercial software or other material to circumvent licensing agreements.

- Users shall not use e-mail to provide unauthorized access to private or confidential information.

- Users shall not use e-mail to provide access to public information without following the existing rules and procedures of the AGENCY for dissemination.

- Users may not encrypt any e-mails without obtaining written permission from their supervisor and their IT Department. If approved, the encryption key(s) must be made known to the AGENCY.

---

[2] *Implementers: For most states, records management authority rests with the state archives or a state records management agency. The state records management authority often sets rules and regulations for local government records, as well.*

[3] *Implementers: Include here the legal definition of a record and offer commentary as appropriate to help users distinguish between records and non-records.*

- Users are reminded that access to and use of the Internet, including communication by e-mail, is not confidential. Users shall not use e-mail to transmit sensitive information unless the e-mail is sent using approved security techniques.[4]

- Users shall not use another user's e-mail account without the permission of the account's owner. Unless specifically acting as an agent for another when sending a message from another account, users should clearly identify themselves as the author of the e-mail message.

- Users shall take reasonable precautions against exposing the system to viruses received through e-mail, including the use and regular updating of anti-virus software.

- Users shall comply with the AGENCY'S E-MAIL/RECORDS retention policy.[5] At least once a month, users shall delete any e-mail and attachments whose retention period has passed. Users shall not delete e-mail (including attachments) that has not met or exceeded the appropriate retention requirements as set forth in the retention policy.

- All e-mail accounts and e-mail messages distributed via the AGENCY'S e-mail service are the AGENCY'S property.

SECTION 5 - QUESTIONS

If you have any questions or comments about this policy, please contact NAME, TITLE, TELEPHONE, and E-MAIL.

If you do not have any questions, AGENCY presumes that you understand and are aware of the rules and guidelines in this e-mail policy and will adhere to them.

SECTION 6 - DECLARATION[6]

I have read, understand and acknowledge receipt of this e-mail policy. I will comply with the guidelines set forth in this policy and understand that failure to do so might result in disciplinary or legal action.

[User's signature]

---

4 *Implementers: Moderate or strengthen this requirement based on your business need and the likelihood of confidential information being intercepted. Note in particular, HIPAA places strict requirements on transmission of medical information over unsecured lines.*

5 *Implementers: If adopted, direct users to the accompanying E-mail Retention Schedule. Otherwise, direct the user to the controlling policy or authority.*

6 *Implementers: If the workforce is unionized, signature of such statements may be resisted because the terms may be regarded as an amendment to the current terms and conditions of work. Because some (but not all) legal opinions hold that these terms need to be collectively bargained, if the workforce is unionized, the Agency should consider handing out the policies without a signature line; a separate document could be signed to indicate receipt of the policy.*

This page left blank intentionally.

MODEL E-MAIL RETENTION SCHEDULE

The vast majority of e-mail messages have only transitory value to the agency and should be discarded after being read. However, some messages remain useful to the agency's business for a period of time because they have reference, legal, administrative, functional, or policy/programmatic (archival) value.

An initial evaluation indicates if messages may be discarded immediately or if they must be retained for a period of time. Messages that are not immediately deleted should be filed with related records and retained in accordance with an approved records retention schedule.

An e-mail message's value is based on its content. This document describes a number of factors that influence a message's value. It identifies:

- Messages of no value that can be deleted immediately. Most messages will fall into this category.

- Messages of limited value that should be kept for a period of time. A relatively small percentage of messages will fall into this category.

- Messages of enduring value that should be kept permanently and are typically deposited in the state archives. Very few messages will be considered permanently valuable.

GENERAL NOTES ON RECORDS RETENTION PERIODS[7]

- Because of the diversity of messages received via e-mail, it's impossible to set a single retention period for all e-mail messages. E-mail messages should be discarded or retained on the basis of their content.

- Consult with the agency's records officer[8] before destroying any message you believe may be of exceptional importance, even if the message's retention period has passed. It is possible that a specific message normally scheduled for destruction should be kept longer because it contains information about an important event or because the message may be relevant to impending litigation. Such messages often relate to current, high profile issues.

- Retention periods apply to both sent and received messages. If you are the sender of a message, your copy is the record copy, and you have primary responsibility for discarding or retaining the message properly. If you have received a message that was sent by another employee, the sender holds the record copy. If you have received a message from someone

---

7 *Implementers: Retention periods listed here are suggested guidelines. Any retention period listed on official records schedules established by your state or agency supersede the periods suggested here. Your agency should identify any record series that must be routinely kept longer than three years (administrative value) and establish procedures for filing and disposing of those records, either by creating an additional retention classification or by extending the basic retention period to include those records.*

8 *Implementers: The agency should identify someone to whom employees can turn with questions about the value of records. That individual should have the knowledge to base decision to keep records on their value rather than deciding to keep records 'just in case.' In the absence of a trained records manager, the person may be a lawyer, accountant, or other administrator.*

outside the system, your copy of the message as received is the record copy. If several people inside the agency have received the same message from someone outside the system, the individuals who respond should keep the original as a record copy.[9]

- You may delete the electronic copy of any message, if you have made a record copy by printing the message or transferring it to another system for preservation. The printed copy of the message must include information about the distribution of the message, including – minimally – the sender, the specific recipients (not just names of distribution lists), the date sent, and any attachments.[10]

- Deleting a message is not equivalent to throwing away a piece of paper. In many systems, a deleted message is moved to a folder named trash, where it can be retrieved until the trash folder is emptied. Emptying the trash is no assurance that a message is completely gone; it may persist in another user's system or on system backup tapes.[11] This persistence of messages has significant implications in case of discovery. Unless the records manager and systems administrator fully understand the many places relevant messages may exist – especially in places they might not think to look, such as trash folders and system backup tapes – they may fail to produce all relevant messages, with significant consequences, if a judge feels there has not been due diligence.

TRANSITORY (EPHEMERAL) VALUE

For most people, the vast majority of messages are of limited value to the organization, often because the messages are duplicates (the record copy is kept elsewhere) or because the messages contain no documentation of decisions or information, which serves as the basis for an action taken.
Examples of messages with transitory value include:

1. Personal messages unrelated to agency business (e.g., invitations to lunch, jokes).

2. Electronic copies of messages printed and filed.

3. Spam (unsolicited, commercial e-mail not directed to you individually).

4. Messages to or from e-mail distribution lists (Listserv) not directly relating to agency business.

5. Copies of publications.

6. Routine requests for information or publications.

7. Letters of transmittal that add no information to that contained in attachments. However, retain the message if it may be necessary to prove time of receipt.

---

9 *Implementers: Clarify who may immediately discard copies of messages received from outside the system based on agency policy. For example, "Individuals cc'ed on a message may delete the message if a principal recipient is responsible for responding to this type of message."*

10 *Implementers: Give specific instructions here on how to print and file messages and attachments to capture sufficient contextual information.*

11 *Implementers: Rotation of backup tapes and disaster recovery copies should be coordinated with retention schedules to avoid copies of messages surviving significantly beyond the date deleted from the system.*

8. Informational messages that do not serve as the basis of action or decisions, such as announcements relating to holidays, charitable appeals, bond campaigns, etc.

9. Received copies of messages sent *from within the agency* and preserved by the sender, especially messages addressed to several recipients. In rare instances, it may be wise to keep the copy you received as proof of receipt or because you don't have confidence that the sender will keep the original copy. For example, the recipient should keep a harassing message, as the sender might delete the sent copy and deny the charge.[12]

Suggested Retention

0–30 days, no destruction notice necessary.
Delete both message and any attachments.

Note: Messages of the types described above may be maintained longer, if they have on-going value for reference and must be retained longer, if they have administrative, legal, functional, or programmatic value.

REFERENCE VALUE

A message that duplicates the official record copy, but which is kept in electronic format for convenience of use or editing. For example, a message from a list server with instructions on how to post or unsubscribe, or a message that is used as a template for routine updates.

Suggested Retention

Indefinite. Delete when of no further use.

LEGAL VALUE[13]

Messages sent from within the agency or received from outside the agency that may help the agency successfully defend itself against litigation actions, enforce its rights, or meet other legal obligations and needs, including compliance with statutes or regulations.

Suggested Retention

It is imperative that all potentially relevant messages – incriminating or exculpatory – are not destroyed once the possibility of litigation is recognized. Because these messages may be found in your in-basket, out-basket, trash box, or other folders created to organize messages, consider

[12] *Implementers: This section is based on two assumptions. First, that it is relatively easy for a recipient to get access to the sent copy for reference and that senders will properly manage their sent messages. Revise or delete this section if those assumptions are not applicable to your agency.*

[13] *Implementers: This section applies to most employees. If the agency has a legal staff, they should develop separate retention guidelines that reflect the records retention demands of attorney-client relationships.*

transferring them to a new folder to ensure that retention periods applied to other folders do not trigger premature destruction.

It may be preferable to print e-mail messages so that they can be kept with the rest of the case files. When printing e-mails for evidence, it is essential that the print copies include the headers to document when messages were sent and received, and all recipients (including cc: and bcc:). Consult with the appropriate legal or records management authority for the preferred method for managing relevant messages.

Minimally, retain messages until any litigation is settled and time for appeals has expired. Then reappraise messages and related files for disposition. Litigation often makes records normally scheduled for destruction good candidates for permanent retention in the archives.

ADMINISTRATIVE VALUE

Messages that facilitate the day-to-day operations of the agency or which are sent from within the agency or are received from outside the agency in the routine course of administering programs. To the extent that the message serves as the record of distribution of important business (minutes, policy changes, etc.), the message may have administrative value independent of the value of the message content.

Examples of messages with administrative value include:

1. Originating copies of correspondence of a repetitive or routine nature.

2. Originating copies of intra-agency correspondence.

3. Originating copies of activity reports summarized in annual reports. *Note: In the absence of summary reports, it may be appropriate to retain these reports permanently.*

4. Originating copies of minutes of routine meetings.

5. Work assignments and duty rosters for office staff.

6. Daily activity reports. *Note: Some reports – especially those containing quantitative data formatted for analysis – may have long-term reference value for trend analysis and should be kept permanently, if a record copy is not kept elsewhere.*

7. Budget reports that are summarized in a larger report.

8. Unpublished calendars of activities and events.

9. Calendars, appointment books, schedules, logs, diaries, and other records documenting meetings, appointments, telephone calls, trips, visits, and other daily activities of employees. *Note: Such records of high-level officials often have significant value and should be kept at least three years after leaving their position.*

10. Messages relating to personnel issues.

Suggested Retention

Delete after three years. No destruction notice necessary.

Note: Financial records may be deleted after a successful audit. Individuals with significant numbers of financial reports may wish to create sub-groups to facilitate destruction of obsolete reports.

FUNCTIONAL VALUE

Messages sent from within the agency or received from outside the agency that are created as the result of a well-defined activity (business process) with similar, if not identical, content and format, and which may be filed as a series. Includes case files, transaction files. May include personnel files.

Examples of messages with functional value include:

1. Activity records (client case files, transactions).
2. Messages of a non-routine nature relating to a specific transaction.

Suggested Retention

Follow records retention schedule for that activity.[14]

POLICY AND PROGRAMMATIC VALUE

Messages sent from within the agency or received from outside the agency that relate to the agency's policies and programs. These messages are evidence of management decisions that affect the agency's work, including the development, modification, or termination of policies or programs.

Examples of messages with policy or programmatic value include:

1. Originating copies of organizational charts and mission statements.
2. Minutes of governing boards, advisory groups, ad hoc committees, or work groups developing programs. See also routine meeting minutes under Administrative Value.
3. Originating copies of messages regarding policies, procedures, general orders governing the operation of the agency.
4. Originating copies of messages regarding policies or programs, including circular messages, directives, or similar information directed to subordinates.
5. Originating copies of messages relating to significant events relating to or affecting a policy or program.
6. Record copies of annual summary reports on program activities, achievements, or plans. May be routine or ad hoc, narrative or statistical.

[14] *Implementers: If no retention schedule exists, develop one.*

7. Record copies of messages regarding studies or reports regarding agency operations.

Suggested Retention

Permanent.

TABLE OF CONTENTS

SECTION 1 – INTRODUCTION AND PURPOSE

Every day, millions of e-mail messages are sent within the United States. At different times, you may feel like all those messages are in your in-basket when you come to work.

Many people use e-mail instead of the phone, especially because e-mail can be a lot less frustrating than playing phone tag. While the informal content of phone conversations and e-mail messages are similar, there's a significant difference. E-mail creates a persistent document, a record of the "conversation."

Most people aren't sure what to do with their e-mail when finished reading it. Many people leave messages they've read in their in-basket because they might want to refer back to them at some point. In reality, though, few messages are ever looked at a second time.

Keeping your old messages in the system can create a number of problems. An enormous number of useless messages can make it hard to find important messages. These messages can clog a system, making it slow to read messages. Finally, useless messages consume disk space; even though disk space is fairly cheap, the increasing number of messages and users can have a real impact on hardware costs, backups, and IT staff.

Another, more subtle problem results from the fact that e-mail creates records of the "conversation." Messages can come back to haunt you. Because e-mail has the familiarity of a phone call, many people make inappropriate statements that would be embarrassing – and possibly incriminating – if made public. You might deny the content of a phone conversation or argue that the content was misunderstood. But, because e-mail messages persist after the conversation, it's more likely that someone else may see them. Because e-mail messages are subject to open records laws, it's even more likely that your old messages may become public.

One of the most ubiquitous questions in the current office place is, "How do I manage my e-mails?" Best practices for managing e-mail are still evolving, in part because e-mail is still relatively new to the office and also because software changes require people to re-learn ways to manage their e-mail.

This document gives guidelines on when e-mail is (and is not) an appropriate means of communication, and suggests ways to use e-mail appropriately when discussing sensitive subjects. It also suggests techniques to manage e-mail by:

- Identifying those messages that are useless and can be deleted.
- Identifying those messages that are important and should be saved.

- Describing ways to organize and store those important messages.
- Determining how to dispose of important messages when they're no longer useful.

SECTION 2 – APPROPRIATE USE

Not all business is appropriate for e-mail. Because e-mail cannot communicate tone of voice or body language, a sender's intended meaning may be misinterpreted. I 5 T2Eos-13(itiv'reatu)-19.4(r)-7.9((fo)-14.4(r)-7.l. c(s-11(

address key people individually – apart from the distribution list – to document when you sent it to them.

Most e-mail programs allow you to create a signature file containing a standard closing that can include your name, title and agency. Including contact information (address, phone number, fax number, e-mail) is a courtesy, saving recipients time looking up this information if they want to contact you by another means.

Representing yourself as someone else by signing his or her name is clearly fraud. If circumstances dictate that you use another person's e-mail account, it is imperative that you clearly identify yourself at the beginning of the message so that recipients understand the message is not from the individual whose account you are using.

The degree of formality is relative to the business at hand and the nature of the relationship. If you have frequent communications with an individual, salutations and closings are less important.

Use a meaningful subject line.
Thoughtful subject lines help recipients distinguish important e-mail; 'You might be interested in this,' might be confused with spam or virus-propagated messages. Good subject lines also aid filing and retrieving messages; 'Here's what you asked for,' is meaningful at the moment, but offers no clue as memory fades over a few days. Finally, good subject lines can help recipients distinguish spam and virus-laden messages from legitimate business.

Include the content of messages received when responding.
Capture the whole of an extended conversation, rather than giving a response in isolation. Use complete sentences when responding to a message, even when including the original text; single word or short phrases are almost always ambiguous to the reader, no matter how clear in the sender's mind.

Messages sent from a work account may be interpreted as official agency policy or opinion.
Unless authorized to speak for the agency in an official capacity, messages should clearly indicate that the message reflects the sender's opinions and ideas, or are drafts for discussion. It may be wise to include a disclaimer such as, "This message reflects the thoughts and opinions of the sender and does not necessarily reflect the official position of AGENCY."

Work-related e-mails sent in your official capacity from a computer outside the system must be transferred to the agency's files for proper retention and disposition.
You may print the message or may transfer messages by forwarding or copying messages to your work account.

Discussion documents should clearly be labeled as drafts.
Such disclaimers are particularly important if the contents of the message could be misinterpreted out of context. For example, a devil's advocate argument could be mistaken as the sender's point of view unless the message explicitly indicates otherwise.

Respect the privacy and confidentiality of individuals who send you e-mail.
Messages – especially those containing personal information – may be forwarded or shared only with other agency employees who are authorized to read such messages, or with the permission of

the original sender. Messages should be shared only when necessary to conduct the business at hand.

Messages containing confidential or sensitive personal information[15] should only be sent via e-mail if the system is known to be secure. Federal law (HIPAA) requires health medical information to be encrypted before being sent over the Internet.

Comply with the e-mail retention policy.
You should manage your e-mail messages by disposing of records in accordance with the AGENCY'S retention policies and schedules, and by properly filing those messages that must be retained. Supervisors are expected to review your e-mail on occasion and to include an evaluation of e-mail use and management as part of your annual reviews.

PERSONAL USE

Brief, occasional messages of a personal nature may be sent and received from a work account, or from a personal private e-mail account if connecting to that account using the agency's equipment or Internet service (e.g., use of a Web browser at work to connect to a Hotmail account). Personal use of e-mail is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action.

Remember that all messages sent from work computers may be considered public records, and that the public has the right to view all messages in the AGENCY's e-mail system, including your personal messages. By using agency equipment or services to send messages, employees expressly waive any right of privacy in anything they create, store, send or receive on the AGENCY's computer system.

Supervisors are expected to see that employee's personal use of the agency's Internet, e-mail, or online services are neither excessive nor improper. If you have any question about the personal use of your work account, or if you are concerned about privacy, use a personal account using your own equipment on your own time.

Personal e-mail sent from a work account should be clearly marked as personal.

Personal use of e-mail or messaging should not interfere with your own or others' work.
Avoid such time wasters as jokes, chain letters, and the like.

Send and read personal messages on your own time, such as breaks or lunch.

Personal messages should not cause the AGENCY public embarrassment.
Avoid messages you would not want to see on the front page of tomorrow's newspaper with your name. In particular, avoid content that have the appearance of illegal, unethical or unprofessional

---

[15] Confidential information includes that information that is restricted by state or federal law. Examples of confidential information include student records (restricted by the Federal Educational Rights and Privacy Act) or medical information (restricted by HIPAA).

Sensitive personal information includes information which is generally unavailable to the public or which is unduly invasive. Examples of sensitive personal information include credit card numbers, unlisted phone numbers, information about prior employment, or financial assets. Information that may be embarrassing, but which is part of the public record, such as a criminal conviction, is not necessarily restricted on the grounds of privacy.

behavior, or which might be conservatively interpreted as overtly biased or sexual. If you receive e-mail that you believe would be embarrassing to the AGENCY, contact your supervisor or the information technology staff.

SECTION 3 – E-MAIL MANAGEMENT AND RETENTION

E-mail and online messages are as diverse as paper letters and telephone calls; they include junk mail, personal notes, and business records. Although they arrive by the same mechanism, the value – and the retention – of the messages depend on their nature.

Although the vast majority of e-mail can be immediately deleted, you should initially presume that all e-mail and messages sent or received using AGENCY's equipment and services – including those of a personal nature – are public records and must be managed in accordance with public records laws.

The AGENCY'S retention schedules and this user manual will help you identify those e-mail or messages that can be legally deleted and those that must be retained. Messages that document business activities and decisions should be kept as long as they are required for business and accountability purposes or as required by law. In some instances, it may be necessary to keep those messages for several years, and a small percentage of messages must be kept permanently.

File your e-mails (with their attachments) and messages so that anyone with need and appropriate authority can find them.[16] In some instances, it may be appropriate to file e-mail or messages within the e-mail program. In other instances, it may be more appropriate to transfer the message (in paper or electronic format) to a paper file or document management program that contains other related records. Follow agency or office procedures for managing e-mail.

AGENCY'S records retention schedule for e-mail (attached) describes common classes of e-mail and indicates how long those messages should be kept. However, messages relating to specific programs received as e-mail must be retained according to the schedules for those programs.

Delete messages of transitory value immediately.
The best practice is to delete or file a message as soon as it is read or sent to avoid building up a backlog that requires time to clean up. In many e-mail systems, deleting a message from the in-basket or out-basket moves it to the trash. The message is not completely erased from the system until the trash is emptied. If you erase messages older than one month from your trash at the beginning of each month, you'll have a chance to change your mind. If you find yourself going back to a message, you may transfer it to an appropriate folder for retention. If you haven't referred back to a message in a month, you probably won't ever need it again.[17]

Destroy only e-mail messages that have met or exceeded the appropriate retention period as indicated on the retention schedule.

---

[16] *Implementers: Describe here the proper way that employees should file their e-mail. For example, you may require that e-mail be transferred to a records management application or to share folders on the server. In the absence of such technology, many agencies require that messages be printed and filed. Another solution – albeit imperfect – would be to require that messages be kept organized within the e-mail reader and that such folders be copied to a server on a regular basis.*

[17] *Implementers: Check to ensure that the month grace period for trash is accurate for your system and make appropriate changes (to the system or this document) so that users know the limits of the system.*

Remember, though, that the electronic copy of any message may be deleted if a record copy has been made by printing the message or by transferring it to another system. The preserved copy of the message must include information about the transmission of the message, including – minimally – the sender, the specific recipients (not just names of distribution lists), the date sent, and any attachments.

Use folders to organize messages that must be saved.
As much as possible, messages should be organized into folders using the same system as equivalent paper files. Folders should be assigned retention periods in accordance with the agency's retention schedule. Employees should periodically (monthly, quarterly, annually) review the contents of folders and delete messages that have passed their retention period. To simplify this process, consider appending the retention period to the end of the folder name. For example, AdminTeam_Minutes_3YR.

Transfer messages out of e-mail systems if the size grows unmanageable.
If the number or size of folders grows too large, transfer messages to near-line or off-line media, or print and file messages when no longer needed for reference or operational purposes. Messages that are no longer current but must be kept permanently should be transferred out of the system by printing or transferred to stable media.

Messages that are potentially relevant to litigation should be preserved, even if their retention period has passed.
Consult with your records coordinator or attorney to determine when it is appropriate to dispose of these messages.

SECTION 4 – SECURITY, ENCRYPTION, AND VIRUSES

A number of factors can compromise the security of e-mail and on-line messages. Many breaches of security are the result of simple human error. For example, a confidential message might be addressed to someone not authorized to see the message. If a workstation is left unattended, unauthorized users can read or send messages they are not allowed to see.

It is possible for e-mail and messages to be intercepted during transmission. Such breaches in security are not common because they require a certain level of technical sophistication and opportunity. Nevertheless, the risk is real.

Access to and use of the Internet, including communication by e-mail, is not perfectly secure.
Consider another means to send messages containing highly sensitive information.

Label messages containing confidential or private information.
Messages from many professionals (lawyers, doctors, clergy) should be labeled clearly at the head of each message, "Privileged and Confidential [Profession]-Client Communication." Optionally, employees may want to include the following notice:

> This message contains information that may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy, or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by e-mail and delete the message.

Use encryption only when authorized by the agency.
E-mail and messages can be encrypted to protect them from being read by unauthorized individuals. However, storing messages in encrypted form runs counter to open records laws and prevents the agency from its legitimate right to review all messages on its system.

Install anti-virus software and update virus definitions at least every other week.
Computer viruses are more and more prevalent in today's world. They can cause considerable damage to a computer or an entire network. An infected computer may not be readily identified, even though damage may be occurring. The utmost care must be taken in adhering to strict anti-virus precautions.

Do not activate programs or open files that have been attached to an e-mail message.
Attachments from a known, trusted source may be opened with caution. Because some e-mail virus programs can make it appear an infected message or attachment has been sent from a known source, you should not activate programs or open files that have not been checked by anti-virus software. Be wary of *any* message from *any* source that contains a subject line that is not clearly related to business or that is ambiguous.

SECTION 5 – QUESTIONS

If you have any questions or comments about this e-mail user manual, please contact NAME, TELEPHONE, and E-MAIL.