North Carolina Department of Cultural Resources

Division of Historical Resources

Archives & Records Section

Government Records Branch

E-mail as a Public Record in North Carolina: A Policy for Its Retention and Disposition

Revised July 2009

Table of Contents

1 General Policies

1.1 Purpose of this E-mail Policy

Increasingly, public employees rely on electronic mail (e-mail) as a quick and useful communication tool for carrying out government business. Employees regularly use the e-mail system to carry out daily activities such as sending and receiving reports, policies, official memoranda, and correspondence, and for supporting various other business-related processes and transactions of their agency.

Like paper records, certain e-mail messages have administrative, fiscal, legal, reference, and/or archival value. These State records may contain evidence of a particular action, have information that protects the rights of individuals or the government, document decisions made during the course of state business, or have lasting historical or cultural value. Therefore, some e-mail messages must be kept as a record to satisfy agency needs, record-keeping requirements, and to comply with the law.

While e-mail system administrators are responsible for system security and performance, individual users are responsible for managing state records effectively and efficiently, regardless of the technology used to create the records.

This policy and corresponding guidelines serve several purposes. The policy ensures that records created, sent, and received through the e-mail system are managed in agreement with the established legal requirements for creating, maintaining, and disposing of all government records. It helps users to classify e-mail messages and make them available for public information requests, and provides guidance on how to retain and dispose of e-mail messages to satisfy business needs, programs, and record-keeping requirements. The guidelines promote best practices and offer ideas and suggestions that can help in the effective management and retention of electronic messages as public records.

1.2 Key Definitions

The term "e-mail" can be confusing because it can mean the e-mail system, the messages distributed by the system, and the act of sending or receiving e-mail messages. For the purpose of this policy ***e-mail systems*** allow computer users to create, send, receive, and store e-mail messages, graphics, and sometimes sounds and animated images over a computer network. The NCMail Service is one of the systems that provide e-mail accounts to government employees through their agencies or departments.

An ***e-mail message*** is a single electronic mail message. The user composes a message using a software application such as Microsoft Outlook. The message often contains a header (or information about the sender and receiver), body (including the content of the message, signature and applicable disclaimers), and attachments. An e-mail message is not a secure communication and is similar to sending a postcard using conventional mail.

Additional definitions are in Appendix 1.

1.3 Ownership of E-mail Messages

Any records including e-mail messages created, received, and/or used on computers or mobile/portable computing devices owned or operated by the State or local counties and municipalities *are government property* and do not belong to you, other employees, or any third parties.[1] Accordingly, public employees who use government information systems should have no expectation of privacy unless expressly granted by their agency or local government.[2]

1.4 Staff Who Telework or Travel

Public employees who have been approved to telework or use mobile/portable computing devices must comply with all information technology security policies, including the agency and statewide acceptable use policies, as applicable. To ensure proper recovery and restoration of data files, offsite employees with laptops or other mobile/portable computing devices are required to back up their information including e-mail messages daily or as soon as practicable. When a mobile/portable computer is outside a secure area, the backup medium must be kept separate from the mobile/portable computer.[3] Please consult with your information technology (IT) department to help with this process. If you have a personal mobile device, you should not forward your work e-mail to it, as work data is then stored on a personal device and is susceptible to potential security risks. Please consult with your information technology department before using a personal mobile device for work.

1.5 Use of Personal E-Mail Accounts

Due to the challenging nature of capturing the information in personal e-mail accounts (such as Gmail™ or Yahoo™), the use of these accounts to conduct official government business is strongly discouraged. If a personal e-mail account is used for government business, employees are required to forward all e-mail messages to their government e-mail account. Those employees who do not have a government e-mail account are expected to print those e-mail messages following the terms of a records retention and disposition schedule. Executive Branch employees who conduct State business via personal e-mail accounts shall ensure that all public records are retained in accordance with Executive Order 18 and are retained pursuant to the Public Records Law and applicable record retention schedules.[4] Members of governing boards who use personal accounts to conduct business manage their e-mails according to the records retention schedules and forward the message to the board's official record keeping entity. If someone has not been appointed, we encourage you to identify the appropriate entity.

1.6 Use of Alternate Technologies

Public employees may not use Instant Messaging (IM) or other alternate technologies unless the risks have been identified and appropriate risk mitigation measures have been implemented or an approved deviation from the Security Manual standard has been obtained from the State Chief Information Officer.[5] If an employee has been approved to use an alternate technology, all messages created, received, or sent using IM, Short Messaging Services (SMS), mobile e-mail

[1] Modified from the DCR Policy Regarding the Use of the Internet and the Use and Privacy of Electronic Mail (September 1, 1999).
[2] State of North Carolina Statewide Information Security Manual – Chapter 2, Standard 020109.
[3] Security Manual – Chapter 3, Standard 030602.
[4] Executive Order No. 18 (issued July 7, 2009).
[5] Security Manual – Chapter 3, Standard 030319.

devices (such as BlackBerry™) or other alternate technologies during the course of government business are to be managed with the same care as e-mail messages, which includes activating the audit log and forwarding all e-mail messages to their government e-mail account. All messages created, received, or sent using alternate technologies are subject to the rules outlined in this e-mail policy.

Employees at local agencies should consult with their IT department to determine use of alternate technologies.

1.7 Policy Review and Updating

To ensure that this policy is current and relevant, it will be reviewed and updated as needed. This includes any updates resulting in the selection and implementation of the e-mail archive system as described in Executive Order No.18.

2 Managing E-mail Messages as Public Records

2.1 Classifying E-mail Messages

Certain e-mail messages, including those with attachments, have administrative, fiscal, legal, reference, and/or archival value. As such, they must be kept as a record to satisfy agency needs, record-keeping requirements, and to comply with the law. However, not every e-mail message that enters or leaves the e-mail system is a public record as defined by North Carolina General Statute (N.C.G.S.) 132. Some e-mail messages may be public records but may also be considered confidential by statute and should be treated accordingly (see Sections 3 and 5.4 for specifics). It is the employee's responsibility to classify and manage e-mail messages in accordance with their records retention and disposition schedule.

An e-mail message is considered to be a ***public record*** when made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. North Carolina General Statutes (N.C.G.S.) §121-2(8) and §132-1(a) provide the following definition:

> "Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, artifacts, or other documentary material, ***regardless of physical form or characteristics*** [emphasis added], made or received pursuant to law or ordinance or in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.

Some examples of e-mail messages that are public records and therefore covered by this policy include:

- policies or directives;
- final drafts or reports and recommendations;
- correspondence and memos related to official business;
- work schedules and assignments;
- meeting agendas or minutes;
- any document or message that initiates, facilitates, authorizes, or completes a business

transaction; and
- messages that create a precedent, such as issuing instructions or advice.

If an e-mail message is not created or received as part of the business of government, it is considered to be ***non-record*** material. Examples include:

- ***Personal messages*** are those received from family, friends, or work colleagues which have nothing to do with conducting daily government business. E-mail accounts may be used for limited family or personal communications so long as those communications do not interfere with their work.[6] Employees subject to Executive Order No. 18 should have no expectation of privacy in their electronic correspondence, and all employees shall assume that information on the State's e-mail system is subject to public review.

- ***Spam*** is electronic junk mail and is similar to the advertising mail received at home. It is completely unsolicited and unwanted and is clearly not related to the transaction of state business, therefore it is considered to be non-record material. While there are tools and techniques for restricting the amount of spam received, there is currently no way to keep it out completely without interfering with the ability to receive important messages. See Section 4 "Technical Security" in the Guidelines for the handling and disposal of spam.

- ***Unsolicited e-mails*** are messages that may be unwanted, but are somewhat business related. These could include non work-related e-mail messages from coworkers such as miscellaneous news articles, non-work related announcements, etc. As with personal messages, these should be deleted in a timely manner.

See Section 1 "Creating E-Mail Messages" in the Guidelines for practical approaches for composing proper business e-mail messages.

2.2 Managing Retention and Disposition

As public records, e-mail messages are subject to the same retention and disposition requirements as records in another format or medium, such as paper or microfilm. Consequently, public employees in both state and local government who use e-mail as part of their work are responsible for keeping or destroying messages following the terms of a records retention and disposition schedule. Employees can refer to their agency's records retention and disposition schedule, the General Schedule for State Agency Records, or the Retention and Disposition Schedules for Counties and Municipalities for specific details. Please consult the Government Records Branch Web site at www.records.ncdcr.gov for schedules and additional information.

Public employees are required to be familiar with and comply with all applicable record-keeping practices and responsibilities mandated by their agency, the State CIO, their records retention and disposition schedules, or other official guidelines or policies to understand e-mail's function in relation to carrying out those duties. Should an agency or local entity lack an approved records retention and disposition schedule, it may not destroy or otherwise dispose of any records in its custody, whether in electronic, paper, or other format (including electronic mail), which are not so authorized by one of the schedules referred to above.[7] Please contact the Government Records Branch of the Archives and Records Section for assistance.

[6] Executive Order No. 18 (issued July 7, 2009).
[7] Public Records with Short-Term Value. http://www.records.ncdcr.gov/guidelines.htm#short.

The content of the e-mail message, the reason it was created, and the administrative, fiscal, legal, and/or historical value of the message to the agency determines what kind of record it is. E-mail messages may have one of three different values depending on the content and function of the message to the agency. Please note that public employees of Executive Branch agencies are subject to additional retention and disposition policies (see item numbers 5 and 11 in Appendix 2) as outlined in Executive Order No. 18.

1. **Short-term records** are temporary in nature. Most e-mail messages fall into this category. Some examples of these types of messages are communications received from professional listservs and broad announcements received by all employees. They have no significant value to an agency for documenting policy, establishing guidelines or procedures, or verifying transactions.

2. **Long-term records** have significant value to the agency but do not need to be maintained permanently. The retention value is generally determined by assessing the record's administrative, fiscal, or legal value.

3. **Permanent records** are records that have lasting historical value because they document or constitute evidence of state policies, decisions, procedures, and essential transactions.

Once it has been determined that an e-mail message is a record that needs to be retained, it needs to be organized and stored until it is ready to be transferred to a repository authorized to appraise, preserve, and provide access to those e-mail messages.

See Section 2 "Managing Your Inbox" in the Guidelines for practical approaches for managing, storing, and organizing e-mail messages. Also see the NC E-mail Retention Checklist (http://www.records.ncdcr.gov/erecords/Emailchecklist.pdf) for additional tips on which e-mail messages to retain.

2.3 Backups

As part of the e-mail infrastructure, the Office of Information Technology Services (ITS) performs regular e-mail system backups for those state and local government agencies participating in the e-mail shared services in order to aid in the restoration of records to the message store and to provide business recovery capability. ITS will procure an e-mail archive system to preserve e-mail messages as soon as practicable and provide that system to all agencies for which it provides e-mail services.[8] Agencies not using ITS's shared services will be expected to secure an e-mail archiving program in order to be compliant with Executive Order No. 18.

E-mail messages stored in folders not on the NCMail server are not subject to the backup cycle. Employees need to perform backups on the messages filed on their hard drive or make arrangements to store those files on their agency server to protect from system failures, unintentional deletions, or tampering. Teleworkers or those employees who use mobile/portable computing devices must download their messages to the agency's network drives daily.

[8] Executive Order No. 18.

For local employees or employees of state government agencies who do not participate in the e-mail shared service, consult with your office information technology staff regarding the back-up and recovery cycle. E-mail messages stored in folders not on the government server are not subject to a backup cycle. Employees need to perform backups on the messages filed on their hard drives or make arrangements to store those files on their agency server. Please note that e-mail messages sent and received by public employees of the Executive Branch agencies are subject to additional backup requirements (see item number 8 and 9 in Appendix 2) as outlined in Executive Order No. 18.

2.4 Preservation

Employees responsible for the long-term preservation of public records should consult with the North Carolina Department of Cultural Resources (DCR) staff to select acceptable media that will protect the integrity of data stored on those media as long as the data are kept.[9] DCR diligently continues to address the challenges of preserving electronic mail over their life-span so they can remain usable and authentic for future users.

See Section 2 “Managing Your Inbox” in the Guidelines for practical approaches for preserving e-mail messages for long-term use.

3 Access to E-mail Messages

E-mail messages are public records that are open and accessible to the public under the same conditions as all other types of government records, provided they do not contain confidential information. Therefore, all employees must assume that all non-confidential information on government e-mail systems is subject to public view and to review by state officials.[10]

Confidential information is protected by the North Carolina General Statute §132-1.2 or other applicable statutes and, as such, must not be disclosed. If e-mail messages contain both confidential and non-confidential information, and a public records request is received, an employee must provide access to the non-confidential information and redact the confidential information from the message. For additional details on the types of information considered to be confidential, see *Laws Relating to Confidential Records Held by North Carolina Government* (http://www.records.ncdcr.gov/guides/confidential_publicrec_2009.pdf).

The following groups have access to e-mail messages:

1. Senders and recipients of electronic mail in the course of normal usage of electronic mail systems.

2. Supervisors of employees who are senders or recipients of electronic mail.

3. Administrators of electronic mail systems or network systems within the Department or other systems employees only (1) as required by the operation of the electronic mail, network, or other computer systems, (2) as requested by supervisors of the senders or recipients, or (3) when there is a reasonable inference that there has been a violation of any proscriptions in this policy.

[9] Statewide Information Security Manual – Chapter 3, Standard 030605.
[10] Executive Order No. 18.

4. Any individual may request access to public records through procedures defined in N.C.G.S. §132-6 by application made to the legal custodian of the record as defined in N.C.G.S. §132-2 and §132-6. The "legal custodian is the "public official in charge of an office having public records," and "does not mean an agency that holds the public records of other agencies solely . . . to provide data processing." Legal custody of electronic mail rests with the office of the sender or recipient.[11]

Consult with your agency or office regarding procedures that are established regarding responses to public records requests. Confidential information protected by statute must not be released.

Because access to e-mails is not limited to the sender only, each e-mail message sent by public employees must include the following statement (or some version of it):

> *This message and any response to this message is being sent on a state e-mail system and may be subject to monitoring and disclosure to third parties, including law enforcement personnel.*

3.1 Confidentiality

An e-mail message having confidential information should not be shared unless proper, formalized security precautions have been established.[12] If you are required to provide records as a result of a public records request, you must securely remove any confidential or privileged information from the records before releasing them. This could include:

1. Information covered by HIPAA (Health Insurance Portability and Accountability Act), including health care, medical records, treatment, and billing information.

2. Information covered by FERPA (Family Educational and Rights to Privacy Act), including student education records.

3. Social Security numbers and other personal identifying information as defined in G.S. § 132-1.10 and §14-113.20.

4. Trade secrets of your agency as defined in G.S. § 132-1.2.

In the above examples, employees are advised to be cautious in using e-mail and, when needed, seek alternative forms of recordkeeping.

4 E-Discoveries

All e-mail messages, including personal communications and other non-record material as described above, may be subject to discovery proceedings in legal actions, investigations, compliance, and audits. All public employees and officials must respond appropriately to any impending action involving e-mail messages. All measures taken in response to an e-discovery action also apply to e-mail messages retained by those working on home computers or using mobile/portable computing devices.

[11] North Carolina Department of Cultural Resources Policy Regarding the Use of the Internet and the Use of Privacy and Electronic Mail (September 1, 1999).
[12] NCMail Policy: 5.

5 Appropriate Use of E-Mail

All e-mail users are expected to know the difference between appropriate and inappropriate use of the e-mail system.

5.1 Responsibility for Appropriate Use

The e-mail system is provided, at the government's expense, to assist employees in carrying out government business. Consequently the e-mail system should primarily be used only to transmit business related information. In addition, employees using the State e-mail system to perform work-related functions shall use the system responsibly and professionally and not make any intentional use of this service in an illegal, malicious, or obscene manner.[13]

See Section 3 "Appropriate Use of E-mail" in the Guidelines for best practices on the appropriate use of e-mail including tips on e-mail etiquette.

5.2 Inappropriate Uses of E-mail

Inappropriate e-mail messages can trigger legal liabilities, lost productivity, negative publicity, and/or damage to an employee's or agency's reputation. Examples of e-mail content that constitute unacceptable use include:[14]

- Private or personal for-profit activities. This includes personal use of e-mail for marketing or commercial transactions, advertising of products or services or any other activity intended to foster personal gain.

- Unauthorized not-for-profit business activities.

- Participation in a *non-business* related listserv. A listserv allows individuals to use e-mail for online discussion. They are typically open to members who subscribe via e-mail and then receive all e-mail messages that are sent to the listserv address.

- Use for political purposes, such as promoting political causes, advancing a political party or a candidate for political office, and expressing political opinions, particularly on controversial issues.[15]

- The use of RSS (Really Simple Syndication) feeds. Using RSS feeds in the course of business is discouraged. If a RSS feed is enabled, all e-mail feed messages must be deleted on a daily basis.

- Use for, or in support of, unlawful/prohibited activities as defined by federal, State, and local laws or regulations. Illegal activities relating to Internet and network access include, but are not limited to:

    - Tampering with computer hardware or software.

[13] State of North Carolina Statewide Information Security Manual – Chapter 10, Standard 100301.
[14] State of North Carolina Statewide Information Security Manual – Chapter 3, Standard 030303.
[15] Adapted from Executive Order No. 18 (signed July 7, 2009).

- Knowingly vandalizing or destroying computer files.
- Transmitting threatening, obscene, or harassing materials.
- Attempting to penetrate a remote site/computer without proper authorization.
- Violating federal and State laws dealing with copyrighted materials or materials protected by a trade secret.
- Sending confidential information without encrypting that information, exposing the data to discovery by unintended recipients.

  Note that this applies to state agencies only. This is considered to be a best practice and local counties and municipalities are encouraged to follow this practice. Local agencies should consult with their IT department to determine uses of encryption.
- Intentionally seeking information about, obtaining copies of, or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users.
- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
- Deliberate interference or disruption of another user's work or system. Users must not take actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance) or the introduction of computer worms or viruses by any means.
- Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities.
- Unauthorized distribution of State data and information. This includes confidential information.

To protect against misrepresentation, all e-mail messages must contain the name of the sender and his or her e-mail address and include the following disclaimer on each e-mail:

Opinions expressed in this message may not represent the policy of my agency.

5.3 Enforcing Appropriate Use

Using government property or funds for personal gain or in any of the examples listed under “Inappropriate Uses of E-mail” is a violation of criminal law and may result in a disciplinary action including dismissal. This includes, but is not limited to, using telephones, equipment,

copiers, fax machines, computers, and e-mail.[16] Additionally, any NCMail user who sends unsolicited advertisements or solicitations, commercial or otherwise, may have their account disabled and be disallowed further service.[17]

6 Technical Security

The security of an e-mail system is a shared responsibility.

For employees participating in NCMail, the ITS shared service, Information Technology Services is responsible for protecting the reliability, availability, and integrity of the NCMail service. ITS uses appropriate security measures to detect security breaches and other violations of system integrity and reviews the security of all network activity, including all NCMail communications, to ensure that use does not violate federal and state laws, statewide policies and standards established by the State Chief Information Officer (CIO).

For local employees or employees of state government agencies who do not participate in the e-mail shared service, consult with your office information technology staff or refer to the service level agreement provided by your e-mail service provider regarding security of your e-mail system.

Individual users should take all reasonable precautions to prevent the use of their e-mail account by unauthorized individuals. Sending e-mail messages to locations outside of the agency/department's local area network may require the use of the Internet for transport, so users should know that the Internet adheres to open standards and is inherently insecure. Users must also assess risk before sending confidential information over an open network. [18]

Employees with state government or local government not using these services need to consult with their IT department regarding rules of use of their networks and security. However, the precautions mentioned above should be heeded to ensure that information and systems remain secure.

See Section 4 "Technical Security" in the Guidelines for practical approaches for identifying security risks and better securing your e-mail account.

7 Staff Departure

When a public employee or official separates from their agency, a hold will be placed on the e-mail account of that individual until the account and computer can be reviewed for record content. Information Technology personnel cannot remove all software from a machine to make it available for use by another user until provisions have been made regarding the records on the machine. Microsoft Outlook stores e-mail messages in a file known as a Personal Storage Table (.pst) files which sometimes reside on a computer hard drive[19]. The .pst files from personal folders created using Microsoft Outlook or other similar files created by other software packages must be addressed and/or saved somewhere for a supervisor to view before the machine can be "wiped" (data erased) and reassigned.

[16] Modified from Office of State Personnel Employee Handbook (issued August 2007): 12.
[17] NCMail Policy: 5.
[18] NCMail Policy: 5.
[19] It is best to have e-mail messages stored on the network so that if something happens to an individual's hard drive the messages are not destroyed inadvertently.

Any e-mail messages maintained on a government owned computer or a mobile/portable computing device must be transferred to the agency or office for review and disposition prior to the last day of employment.

See Section 2 “Storing and Organizing E-Mail Messages” in the Guidelines for practical approaches for storing e-mail messages as a .pst file to your network or hard drive.

8 Training

DCR provides training on managing e-mail as a public record for all employees, both local and state. In addition, it offers training on the Microsoft Exchange e-mail system, the concepts and fundamentals of which can be transferred to other software packages. DCR also offers ongoing training, especially after upgrades or transitions to new e-mail programs and on an as-needed basis.

Please note that public employees of the Executive Branch agencies are subject to additional policies (see item number 10 in Appendix 2) as outlined in Executive Order No. 18. In order to track successful completion of training, it is recommended that upon completion of training, public employees of the Executive Branch print a copy of their training certification and forward it to their Human Resources representative.

9 Relationships with Existing Policies

This policy has been created within the context of the following documents:

- Executive Order No. 18: E-mail Retention and Archiving Policy (issued July 7, 2009)

- General Schedule for State Agency Records (issued August 31, 2006) (http://www.records.ncdcr.gov/schedules/GS_Amendments2006.pdf)

- North Carolina General Statutes (http://www.ncleg.net/gascripts/statutes/Statutes.asp)
    - §14-113.20. Identity Theft.
    - §14-454 (b). Accessing computers.
    - §121-2(8). Definitions
    - §132-1(a). “Public Records” defined.
    - §132-1.10. Social security numbers and other personal identifying information.
    - §132-1.2. Confidential information.
    - §132-2. Custodian designated.
    - §132-6. Inspection and examination of records.

- Office of Information Technology Services Policy Manual – 18.07 NCMail Policy (http://www.its.state.nc.us/ServiceCatalog/documents/18-07NCMail.pdf)

- Office of State Personnel Employee Handbook (issued August 2007) (http://www.osp.state.nc.us/emphndbk/Handbook2007.pdf)

- Public Records with Short Term Value (Guidelines) (http://www.records.ncdcr.gov/guidelines.htm#short)

- Record Retention and Disposition Schedules for Counties and Municipalities (http://www.records.ncdcr.gov/local/default.htm)

- State of North Carolina Statewide Information Security Manual (http://www.scio.state.nc.us/documents/docs_Active/Statewide%20Information%20Security%20Manual/Statewide%20Information%20Security%20Manual%20-%20Searchable%20Version.pdf)

    - Standards:
        - 020109 — Monitoring System Access and Use
        - 030303 — Sending Electronic Mail
        - 030305 — Retaining or Deleting Electronic Mail
        - 030319 — Instant Messaging Communications
        - 030509 — Information Retention Standard
        - 030602 — Backing Up Data on Portable Computers
        - 030605 — Archiving Electronic Files
        - 030708 — Receiving Unsolicited E-mail
        - 030310 — Receiving Misdirected Information by E-mail
        - 030311 — Forwarding E-mail
        - 100301 — Using the Internet in an Acceptable Way

10 Conclusions

E-mail messages should be treated like any other public record. Delete non-record materials in compliance with the provisions of Executive Order No. 18 and keep business-related messages and attachments in accordance with your records retention and disposition schedule. Print or convert to microfilm any e-mail messages and attachments with lasting evidential or historical value. E-mail messages are the same as any other format of public record and must follow the requirements set in retention and disposition schedules. By setting up a practical mailbox folder system, users can simplify the decision-making process and aid in filing and retrieval. Electronic storage also has its own costs. Careful e-mail management will help reduce the stress on that storage and any other associated costs.

As mailboxes overflow with e-mail messages, following the provisions of the records retention and disposition schedule is essential for good records management practices. Realizing that e-mail classification and management is a shared responsibility, the Government Records Branch of the Department of Cultural Resources is ready to respond to requests to clarify these guidelines, offer records and information management training, and help identify which records need to be kept for a specific period.

11 Contact Information for Government Records

For more information, please contact us at:

Department of Cultural Resources
Division of Historical Resources
Archives and Records Section
Government Records Branch
Physical Location: 215 N. Blount Street, Raleigh, N.C.
Main Telephone: 919-807-7350
E-mail: Records@ncdcr.gov
Or visit our **Web site** at http://www.records.ncdcr.gov/default.htm.

Appendix 1 - Definitions

- **Archival value** - the ongoing usefulness or significance of records, based on the administrative, legal, fiscal, evidential, or historical information they contain, justifying their continued preservation. In general, records with archival value are estimated to make up only three to five percent of an organization's records. (Society of American Archivists [SAA] Glossary)

- **Backup** - the copying of data stored on a computer so that it can be restored should the original data be destroyed by whatever cause (mechanical or software failure, theft or disaster).

- **Copyrighted material** – includes materials that may be protected by Copyright Law (for example, a cartoon, article, or excerpt from a book). In other words, if the information or material is copyrighted, it may not be publicly circulated without prior authorization from the copyright holder.

- **Discovery** – the part of the litigation process in which opposing parties exchange relevant documents, testimony, and other information. Litigants generally request and receive information necessary to build a case in preparation for the trial. Discovery helps each side understand the material facts and evidence in advance of the trial. It also prevents anyone from being ambushed at the trial. (*E-mail Rules*, page 125)

- **Disposition** - materials' final destruction or transfer to an Archives as determined by their appraisal. (SAA Glossary)

- **Document** - traditionally considered to mean text fixed on paper. However, a document includes all media and formats. Photographs, drawings, sound recordings, and videos, as well as word processing files, spreadsheets, Web pages, and database reports, are now generally considered to be documents.(SAA Glossary)

- **E-mail message** – a single electronic mail message. It generally contains a header (or information about the sender and receiver), body (including the content of the message, signature, and applicable disclaimers), and attachments. The user can compose a message using a software application such as Microsoft Outlook.

- **Encryption** - the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge.

- **Mobile/portable computing device** – a pocket-sized computing device, typically having a display screen with touch input or a miniature keyboard. These devices include wireless PDAs (Personal Digital Assistants) and handhelds, mobile phones, laptops with wireless capabilities, and e-mail specific devices, such as the Blackberry, designed for business use.

- **Network** - a number of computers connected together to share information and hardware. A Local Area Network (LAN) is small, usually confined to a single building or group of buildings. A Wide Area Network (WAN) is a system of LANs. It is large, with many computers linked.

- **Receiver**- the target of a message in the communication process.

- **Record** - data or information in a fixed form that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference. A record has fixed content, structure, and context. (SAA Glossary)

- **Retention and disposition schedule** - a document that identifies and describes an organization's records, usually at the series level, provides instructions for the disposition of records throughout their life cycle. (SAA Glossary)

- **Sender** - the originator of the message in the communication process; also called the Source.

- **Telework** - permits agencies to designate employees to work at alternate work locations for all or part of the workweek in order to promote general work efficiencies. (N.C. Office of State Personnel Employee Handbook)

- **Users** - all persons whose access to or use of NCMail is funded by the state or is available through equipment owned or leased by the state. (NCMail Policy)

Appendix 2 –Policies Applicable to Executive Branch Employees (*excerpted from Executive Order No. 18*)

5. Executive Branch employees shall not permanently delete any e-mail messages that they **send** for at least 24 hours, and shall not permanently delete any e-mail messages they **receive** for at least 24 hours except that they may immediately and permanently delete any e-mail messages they **receive** that are not clearly related to the transaction of State business, such as e-mails containing advertising materials or offensive materials. After 24 hours, Executive Branch employees shall retain or delete e-mails they have sent or received according to the retention schedules for their agency established by the Department of Cultural Resources.

8. All Executive Branch agencies shall copy all e-mails sent and received by their employees on backup tapes at least once daily. The Office of Information Technology Services (ITS) will provide this backup service to all agencies for which it provides e-mail services. Each Executive Branch agency that does not use ITS e-mail services shall employ a back-up system that creates a back-up copy of the messages in all e-mail systems of the agency at least once daily. All backup tapes created after the issuance of Executive Order 150 and prior to the implementation of a single e-mail archive system will be maintained for 10 years. After implementation of an e-mail archive system, backup tapes will be maintained for such period as ITS may establish.

9. ITS will procure an e-mail archive system as soon as practicable and provide that system to all agencies for which it provides e-mail services. ITS will make this archive system available to other Executive Branch agencies as soon as practicable. E-mails shall be retained in this system for 10 years. ITS will consult with North Carolina Department of Cultural Resources (DCR) to identify e-mails that should be preserved beyond 10 years.

10. DCR shall provide Executive Branch employees with mandatory online training for managing e-mail as public records.

11. DCR shall conduct random audits of State agencies in the Executive Branch to ensure that employees are in compliance with the records retention and disposition schedules.

Bibliography

Flynn, Nancy and Randolph Kahn Esq. 2003. *E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues*. New York: AMACOM (American Management Association).

Kentucky Department for Libraries and Archives*. Guidelines for Managing E-Mail in Kentucky Government.* http://www.kdla.ky.gov/recmanagement/EmailGuidelines.pdf (accessed February 25, 2009).

Moses, Richard-Pearce. 2005. *A Glossary of Archival and Records Terminology*. http://www.archivists.org/glossary/ (accessed February 19, 2009).

New York State Archives. 2008. *Developing a Policy for Managing Email*. Archives Technical Information Series #85. http://www.archives.nysed.gov/a/records/mr_pub85.shtml (accessed February 13, 2009).

Pennock, Maureen. 2006. *Digital Curation Manual. Curating E-Mails: A life-cycle approach to the management and preservation of e-mail messages.* Digital Curation Centre. http://www.dcc.ac.uk/resource/curation-manual/chapters/curating-e-mails/ (accessed February 25, 2009).

State of Kansas. *Managing Electronic Mail Guidelines for Kansas Government Agencies*. http://www.kshs.org/government/records/electronic/email_guidelines_final.pdf (accessed February 14, 2009).