Managing Electronic Records for Community Colleges

Introduction & Brief Overview of Digital Preservation Challenges

Legalities

a. General Statute 121: Archives and History Act
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_121.html

- § 121-4(2): The Department of Natural and Cultural Resources shall have the power to conduct a records management program, including the operation of a records center or centers and a centralized microfilming program, for the benefit of all State agencies, and to give advice and assistance to the public officials and agencies in matters pertaining to the economical and efficient maintenance and preservation of public records.
- § 121-5(b): No person may destroy, sell, loan, or otherwise dispose of any public record without the consent of the Department of Natural and Cultural Resources, except as provided in G.S. 130A-99. Whoever unlawfully removes a public record from the office where it is usually kept, or alters, mutilates, or destroys it shall be guilty of a Class 3 misdemeanor and upon conviction only fined at the discretion of the court.
- § 121-5(c): When requested by the Department of Natural and Cultural Resources, public officials shall assist the Department in the preparation of an inclusive inventory of records in their custody, to which inventory shall be attached a schedule, approved by the head of the governmental unit or agency having custody of the records and the Department of Natural and Cultural Resources, establishing a time period for the retention or disposal of each series of records. So long as such approved schedule remains in effect, destruction or disposal of records in accordance with its provisions shall be deemed to have met the requirements of G.S. 121-5(b).

b. General Statute 132: Public Records
http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132

- § 132-1(a): "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, 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.
- § 132-1(b): The public records and public information compiled by the agencies of North Carolina government or its subdivisions are the property of the people. Therefore, it is the policy of this State that the people may obtain copies of their public records and public information free or at minimal cost unless otherwise specifically provided by law. As used herein, "minimal cost" shall mean the actual cost of reproducing the public record or public information.
- § 132-3(a): No public official may destroy, sell, loan, or otherwise dispose of any public record, except in accordance with G.S. 121-5 and G.S. 130A-99, without the consent of the Department of Natural and Cultural Resources. Whoever unlawfully removes a public record from the office where it is usually kept, or alters, defaces, mutilates or destroys it shall be guilty of a Class 3 misdemeanor and upon conviction only fined not less than ten dollars ($10.00) nor more than five hundred dollars ($500.00).

c. Electronic Records Laws
Public Records Law: Public Inspection of Records
http://www.ncga.state.nc.us/enactedlegislation/statutes/html/bysection/chapter_132/gs_132-6.html

- § 132-6.1(a): After June 30, 1996, no public agency shall purchase, lease, create, or otherwise acquire any electronic data-processing system for the storage, manipulation, or retrieval of public records unless it first determines that the system will not impair or impede the agency's ability to permit the public inspection and examination, and to provide electronic copies of such records. Nothing in this subsection shall be construed to require the retention by the public agency of obsolete hardware or software.
- § 132-6.1(b): Every public agency shall create an index of computer databases compiled or created by a public agency on the following schedule:
  State agencies by July 1, 1996;
  The index shall be a public record and shall include, at a minimum, the following information with respect to each database listed therein: a list of the data fields; a description of the format or record layout; information as to the frequency with which the database is updated; a list of any data fields to which

public access is restricted; a description of each form in which the database can be copied or reproduced using the agency's computer facilities; and a schedule of fees for the production of copies in each available form.

- § 132-6.1(c): Nothing in this section shall require a public agency to create a computer database that the public agency has not otherwise created or is not otherwise required to be created. Nothing in this section requires a public agency to disclose security features of its electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes.

Electronic Commerce Act

- G.S. § 66-58.4: All public agencies may use and accept electronic signatures pursuant to this Article, pursuant to Article 40 of this Chapter (the Uniform Electronic Transactions Act), or pursuant to other law.
- G.S. § 66-58.5(a): An electronic signature contained in a transaction undertaken pursuant to this Article between a person and a public agency, or between public agencies, shall have the same force and effect as a manual signature provided all of the following requirements are met:
  (1) The public agency involved in the transaction requests or requires the use of electronic signatures.
  (2) The electronic signature contained in the transaction embodies all of the following attributes:
  a. It is unique to the person using it;
  b. It is capable of certification;
  c. It is under sole control of the person using it;
  d. It is linked to data in such a manner that if the data are changed, the electronic signature is invalidated; and
  e. It conforms to rules adopted by the Secretary pursuant to this Article.

Uniform Electronic Transactions Act

- G.S. § 66-317(a): A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- G.S. § 66-317(b): A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- G.S. § 66-317(c): If a law requires a record to be in writing, an electronic record satisfies the law provided it complies with the provisions of this Article.
- G.S. § 66-317(d): If a law requires a signature, an electronic signature satisfies the law provided it complies with the provisions of this Article.
- G.S. § 66-318(a): If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if:
  (1) The sender or its information processing system inhibits the ability of the recipient to print or store the electronic record; or
  (2) It is not capable of being accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.
- G.S. § 66-322(a): If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:
  (1) Accurately reflects the information set forth in the record at the time it was first generated in its final form as an electronic record or otherwise; and
  (2) Remains accessible for later reference.

d. 07 NCAC 04M .0510: Methods of Destruction
http://ncrules.state.nc.us/ncac/title%2007%20-%20cultural%20resources/chapter%2004%20-%20archives%20and%20history/subchapter%20m/07%20ncac%2004m%20.0510.html

(a) When used in an approved records retention and disposition schedule, the provision that paper records are to be destroyed means that the records shall be:
  (1) burned, unless prohibited by local ordinance;
  (2) shredded or torn so as to destroy the record content of the documents or materials concerned;
  (3) placed in acid vats so as to reduce the paper to pulp and to terminate the existence of the document or materials concerned; or

(4) sold as waste paper, provided that the purchaser agrees in writing that the documents or materials concerned will not be resold without pulverizing or shredding the documents so that the information contained within cannot be practicably read or reconstructed.

(b) When used in an approved records retention and disposition schedule, the provision that electronic records are to be destroyed means that the data and metadata are to be overwritten, deleted, and unlinked so the data and metadata may not be practicably reconstructed.

(c) When used in an approved records retention and disposition schedule, the provision that confidential records of any format are to be destroyed means the data, metadata, and physical media are to be destroyed in such a manner that the information cannot be read or reconstructed under any means.

Records Retention and Disposition Schedule

http://www.stateschedules.ncdcr.gov/

Agency Level 1: North Carolina Community College System
Agency Level 2: Colleges in the Community College System

Policies

Guidelines for Managing Trustworthy Digital Public Records
http://archives.ncdcr.gov/Portals/26/PDF/guidelines/guidelines_for_digital_public_records.pdf

Sample Electronic Records and Imaging Policy For Use by Local and State Agencies
http://archives.ncdcr.gov/Portals/26/PDF/guidelines/model_erec_policy.pdf

1. Purpose

2. Responsible Parties

3. Availability of System and Records for Outside Inspection
   - Best Practices for Digital Permanence
     http://archives.ncdcr.gov/Portals/26/PDF/guidelines/digital_permanence.pdf

4. Maintenance of Trustworthy Electronic Records

5. Components of Information Technology System
   - Global Shared Storage Guidelines
     http://archives.ncdcr.gov/Portals/26/PDF/guidelines/SharedStorageGuidelines.pdf
   - Best Practices for Cloud Computing
     http://archives.ncdcr.gov/Portals/26/PDF/guidelines/cloud_computing.pdf

6. Documentation of Information Technology System

7. Digital Imaging Program Documentation and Procedures
   - Guidelines for Digital Imaging Systems
     http://archives.ncdcr.gov/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines.aspx#imaging
   - Scanning in State Agencies
     https://ncrecords.wordpress.com/2014/11/24/scanning-in-state-agencies/

8. Other Electronic Records Management Practices
   - File Format Guidelines for Management and Long-Term Retention of Electronic Records
     http://archives.ncdcr.gov/Portals/26/PDF/guidelines/file_formats_in-house_preservation.pdf
   - Digital Preservation Tutorials: File Naming
     http://digitalpreservation.ncdcr.gov/tutorials.html
   - Best Practices for State Agency Social Media Usage in North Carolina
     http://archives.ncdcr.gov/Portals/26/PDF/guidelines/best_practices_socialmedia_stateagency.pdf

9. Compliance and Electronic Records Self-Warranty

Email

Executive Order 18:
https://www.ncdps.gov/cit/executiveorders/EO18.pdf

Strategies for E-mail Retention
https://ncrecords.wordpress.com/2015/01/29/strategies-for-email-retention/

Preserving Email

Short Term	Long Term	Permanent
< 5 years	> 5 years	Permanent
Retain in email client	Recommended to retain in email client only temporarily	Recommended to retain in email client only temporarily
Delete from client when retention has been met	Export message(s), file with other electronic records on agency server, and delete from client after successful export	Export message(s), file with other electronic records on agency server or onto analog media, and delete from client after successful export or media conversion

Short-term records are temporary in nature. Many e-mail messages fall into this category. Examples include communications received from professional listservs and announcements received by all employees. They have no significant value to an agency.

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

Permanent records have lasting historical value because they document 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.

Best File Formats for Long-Term Retention

	Recommended	Acceptable	Not recommended
Multiple Messages	Microsoft Outlook Personal Storage Table (.pst)	MBOX, MIME (.mbx, .mbox)	
Single Messages	Microsoft Outlook Personal Storage Table (.pst)	Email Message, MIME (.eml, .txt), with email header Plain Text (.txt), with email header Rich Text (.rtf), with email header PDF/A-1a (.pdf) (ISO 19005-1 compliant PDF/A), with email header HTML (.html), with email header Microsoft® Outlook® Message (.msg), with email header	Apple® Mail (.emlx), with or without email header Plain Text (.txt) without email header Rich Text (.rtf) without email header PDF/A-1a (.pdf) (ISO 19005-1 compliant PDF/A), without email header PDF, with or without email header HTML (.html) without email header

Electronic Recordkeeping Plan Template
adapted from Kansas Historical Society
https://www.kshs.org/government/records/electronic/RecordkeepingPlanTemplateVer22form.rtf

Agency:
Unit:
Date Plan Completed:

A. File Formats
    1. Identify the file formats used by the system to create and store data.
        a. Are these file formats proprietary?
            i. If so, can the system export the data/records in a non-proprietary format?
                (1) Which formats?
                (2) Has this process been tested?
    2. Can system metadata be exported to XML?
    3. Are images stored in the system?
        a. Are the images stored in a database?
            i. Can they be exported?
            ii. Are the images and associated metadata kept together when exported?
    4. Is the presentation format of the data/record significant to understanding the records accurately?
        a. If so, what procedures are in place to preserve the presentation format?

B. Data Integrity and Authenticity
    1. Describe the records capture and revision processes (e.g., how data is entered into and changed within the system).
        a. Describe any audit trails in place to track the records capture process.
        b. Describe any audit trails in place to track the records revision process.
            i. If legacy data is replaced with new data during the revision process, is there a need to retain the data being overwritten (versioning)?
                (1) If so, what is the process for retaining the legacy data?
    2. What is the process for making and documenting changes to the system itself (e.g., changing a data field)?

C. Data Security, Confidentiality, and Access
    1. Does the system contain any confidential or private data?
        a. If yes, how does the system protect this data?
    2. How will access to private/confidential data in the system be handled?
    3. Describe the process for accommodating public records requests for records from the system?
    4. What audit trails are in place to track the security of the system and to safeguard data integrity and authenticity from unauthorized changes?
    5. Is the data in the system encrypted?
        a. If so, are the encryption keys placed in escrow?

D. System Backup and Recovery

1. How is the data in the system backed up?
    a. Has the backup recover process been successfully tested?
    b. What is the frequency of backup?
2. Is there a disaster recovery plan in place?
    a. Has the disaster recovery plan been successfully tested?
        i. If so, how often is the disaster recovery plan tested?

E. Preservation

1. What storage media is currently used to store backed-up data?
2. Describe plans for refreshing storage media used to store records in the system.
3. Describe the process that will be used to monitor system and storage media obsolescence.
    a. How will decisions be made on when and how to convert or migrate data in the system to new software or hardware platforms?
    b. How will decisions be made on when and how to convert or migrate to new storage media?
    c. How will migrations be checked to verify that the information recorded is not changed in any way when it is copied to new media?
4. If records are not going to be maintained within the active system, how will they be preserved and retrieved during the entire retention period?

Useful Resources from the State Archives

http://archives.ncdcr.gov/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines

- ✓ Managing Electronic Public Records: Recognizing Perils and Avoiding Pitfalls
- ✓ Global Shared Storage Guidelines
- ✓ Best Practices for Cloud Computing
- ✓ Sample Electronic Records and Imaging Policy For Use by Local and State Agencies
- ✓ Guidelines for Managing Trustworthy Digital Public Records
- ✓ Digital Signature Policy Guidelines
- ✓ Best Practices for Electronic Communications Usage in North Carolina: Text and Instant Message
- ✓ Best Practices for Electronic Communications Usage in North Carolina: Guidelines for Implementing a Strategy for Text and Instant Messages
- ✓ Best Practices for State Agency Social Media Usage in North Carolina
- ✓ Best Practices for Digital Permanence
- ✓ Guidelines for Digital Imaging Systems (5 parts)
- ✓ Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition
- ✓ File Format Guidelines for Management and Long-Term Retention of Electronic Records
- ✓ Best Practices for File-Naming
- ✓ Database Indexing
- ✓ Security Backup Files as Public Records in North Carolina; Guidelines for the Recycling, Destruction, Erasure, and Re-use of Security Backup Files

Other Electronic Records Resources

Digital Heritage Center Digitization Guidelines
http://www.digitalnc.org/about/policies/digitization-guidelines/

Managing Electronic Records
http://nagara.org/images/downloads/2012___2013_LG_Records_Management_Bulletins/managing_electronic_records.pdf

Statewide Information Security Manual
https://www.scio.nc.gov/library/pdf/SISM-1-2015.pdf

CONTACT US

Mark Holland, Unit Head	mark.holland@ncdcr.gov	919-807-7358
Courtney Bailey	courtney.bailey@ncdcr.gov	919-807-7368
Kurt Brenneman	kurt.brenneman@ncdcr.gov	919-807-7357
Rashida Felder	rashida.felder@ncdcr.gov	919-807-7364
Kyna Herzinger (Records Management Analyst for NC Community College System)	kyna.herzinger@ncdcr.gov	919-807-7366
Emily Sweitzer	emily.sweitzer@ncdcr.gov	919-807-7360
Jason Woolf, Western Region (Asheville)	jason.woolf@ncdcr.gov	828-296-7230 x224

We will be available to …

- Write records retention and disposition schedules
- Answer questions about records schedules and general records management
- Conduct workshops
- Provide assistance on disaster planning and recovery issues

Website: http://archives.ncdcr.gov/For-Government

Blog: http://ncrecords.wordpress.com/