Electronic Data Retention and Preservation Policy[1]

Purpose and Scope

The purpose of this policy is to:

- Identify the types of College-related electronic information, including the location of the information;
- Identify what departments or individuals are responsible for managing the devices on which electronic information is stored;
- Identify routine electronic content destruction activities;
- Identify electronic information that is not reasonably accessible because of undue burden or cost;
- Outline a mechanism for informing employees of litigation holds that will obligate the college to identify and preserve electronic information; and
- Outline our plan for identifying, collecting, and preserving electronic information in the event of a litigation hold.

The policy applies to all Wofford employees and to all College-related information stored in electronic format by the College and its employees.

- This information includes, but is not limited to, electronic mail, personal calendars, instant messages, word processing and presentation documents, spreadsheets, databases, voice messages, photographs, videos, audio files, information on handheld devices (e.g., PDAs, Blackberry devices, and iPods), web pages, and data in any other location where electronic information can be stored.
- It also includes College-related information stored on personally-owned home computers.

The policy identifies College-related electronic information that must be preserved in the event of litigation, so that it is potentially available for electronic discovery. Preservation of the information does not mean that it necessarily will be made available to an opposing party. Before any information is turned over to an opposing party, Wofford's counsel will review the information for relevance and determine that it is not otherwise protected or privileged.

[1] Primarily based on documents available in the EDUCAUSE resources on ESI and E-Discovery. 24-Feb-07. <http://www.educause.edu/Browse/645?PARENT_ID=822>

Types of Electronic Information

Wofford College electronic information is stored in several different ways.

- The bulk of the College’s electronic information is stored on servers and network storage centrally managed by the Information Technology Department (IT). This information includes, but is not limited to:
    - Email messages and personal calendars that are stored on our Network-Attached Storage (NAS);
    - Personal web pages and electronic files (Word documents, spreadsheets, etc.) that are stored in individuals’ personal network storage on our NAS;
    - Administrative information that is stored by our integrated administrative software system, Banner, on the Banner and Xtender servers;
    - Telephone logs and voice mail messages that are stored on the telephone system servers; and
    - Server and network activity logs that are stored on the servers controlling the activity.
- Some information is stored on individual machines (desktop computers, laptop computers, and handheld devices) and in portable secondary storage.
    - The machines and portable secondary storage may include, but are not limited to:
        - College-owned machines furnished to departments and employees by the College;
        - College-owned computers, such as kiosk machines and classroom computers, that are accessible to the public;
        - Personally-owned home computers, which sometimes are used for College-related business; and
        - CDs, DVDs, external hard drives, and flash memory drives.
    - This information is managed by individuals using the machines and portable secondary storage.
- Some Banner reports are stored on the Business Objects server, which is managed by the Information Management Department (IM). The Business Objects server is located in the IT Data Center and is backed up by IT.
- Library information is stored on servers located in the Library. These servers are managed by the Library staff.
- Digital images are stored on the NAS by the Digital Access Management system (DAM), which is managed by the Communications Department. The DAM system is housed on a server that is located in the IT Data Center and is backed up by IT.
- College web site information is stored in the Content Management System (CMS), which is managed by the Communications Department. The CMS is housed on a server that is located off-campus.
- Residence Hall key information is stored on the Secure Perfect server, which is managed by Campus Safety office. The Secure Perfect server is located in the IT Data Center and is backed up by IT.

- Information required for disaster recovery is stored on backup tapes managed by IT. These tapes are stored both on campus and off-site at a document management facility.
    - IT backs up the servers and NAS in the IT Data Center daily.
    - Daily backup tapes are stored in a building on campus.
    - Once a week, a backup tape is transferred to on off-site facility.

Routine Electronic Content Destruction

1. Centrally-managed electronic information sometimes is regularly overwritten or destroyed in the course of our routine activities.
    - Email messages are deleted from individuals' network mailboxes or moved to individuals' own computers at their discretion. Deleted messages are retained by IT for 30 days following deletion, after which time they no longer are retained and may be overwritten.
    - With the exception of retired faculty and staff, network accounts are routinely deleted four weeks after their former owners have left Wofford.
    - Banner data that are entered routinely using the Banner forms generally do not overwrite existing data, so that a record of routine Banner transactions almost always exists in the system.
        - In a few Banner forms, such as SPAPERS, changes completely destroy any prior data.
    - Banner data that are entered directly in the data tables by the Banner Database Administrator (DBA) at the request of a department do overwrite existing data. Records of such changes are retained on paper by the Banner DBA.
    - Xtender data is not removed automatically. It can be removed at the discretion of users with Xtender maintenance access.
    - Logs of Banner activity are retained for 60 days and then are overwritten.
    - Library catalog information is retained indefinitely, as long as a book remains in the Library catalog
    - Images for Library course reserves are deleted at the end of each semester and then are overwritten.
    - Library book circulation records for individuals are deleted and overwritten when books are returned.
    - Library collection data and statistics are retained for two years and then are deleted and overwritten.
    - Telephone logs are retained for 30 days and then are overwritten
    - Voice mail messages are deleted at the discretion of the user. Undeleted messages are retained for 30 days and then are overwritten
    - Network equipment and server logs are retained for varying time periods and then are overwritten.
        - Intrusion Detection and Prevention server logs are retained indefinitely;
        - Access Control System logs are retained for 6 months; and
        - Network Equipment logs are kept for 4 weeks.

- Server application, security, and system logs are retained for 7 days. Domain controller directory service and file replication service logs also are retained for 7 days. Server logs beyond their retention period are overwritten.
- The Business Objects server holds only the format of reports and does not retain data used for reports
- Digital Asset Management images are deleted at the discretion of staff members in the Communications Department, after which time they may be overwritten.
- The Secure Perfect residence hall database is cleaned up annually when IT adds records for incoming freshmen and purges the records for graduated seniors.
- Information stored in the Web site Content Management System is deleted at the discretion of staff members in the Communications Department, after which time it may be overwritten.

2. Retention of information on individual machines, network storage, and portable secondary storage managed by departments and employees is left to the discretion of the individuals responsible for the information.

3. Backup tapes kept at the off-site facility are retained for three weeks for disaster recovery purposes. After three weeks the tapes are used again and the data on the tapes are overwritten in the process. Backup tapes no longer in use are shredded.

Electronic Information that is Not Reasonably Accessible

Backup or mirroring of systems is done for disaster preparedness purposes only and is not intended to function as a means of data retention. Email messages stored on backup tapes or mirrors are not reasonably accessible because of undue burden or cost. Information that has been routinely deleted, destroyed, or overwritten in accordance with this policy is not reasonably accessible because of undue burden or cost.

Informing Employees of a Litigation Hold

As soon as practicable after receipt of notice or other information that litigation has been or may be commenced, the Senior Vice President(s) in charge of the affected departments will notify in writing the heads of these departments and the Vice President of Technology of a new potential or actual claim. A Notice of Litigation Hold form is supplied for this purpose. The following information will be provided:

- A brief description of the dispute;
- Names of plaintiff(s), defendant(s), and any other known relevant parties and witnesses;
- The departments likely to be involved;
- The claims raised;
- The time period during which relevant events occurred;
- The timeframe for data preservation; and
- Any other information that will help identify relevant material that needs to be preserved.

This notification must be accompanied by a clear instruction to preserve all electronic information related to the matter, including electronic information created before and after the notice is issued. This will be the first step in issuing a litigation hold – an order from the College requiring its employees to preserve information. While the litigation hold is in effect, periodic (monthly) reminders must be sent. Department heads must be instructed that all relevant information must be preserved, by themselves and by their staff, until the department heads are notified by the Senior Vice President(s) in charge that the litigation hold is no longer in effect.

Identifying and Preserving Information in Case of a Litigation Hold

1. IT will take immediate steps to preserve all centrally-managed data, including the suspension of automatic destruction of potentially discoverable data. The general hold will remain in effect until more information is forthcoming about the types of documents that need to be preserved, the timeframe for preservation, the subject matter of the materials, and specific instructions on how to preserve the information.

2. Heads of affected departments will immediately notify potentially involved staff members to preserve any and all data that may be relevant to the litigation. This order will remain in effect until steps have been taken to identify the specific set of data that must be preserved.

3. As soon as possible following notification by the Senior Vice President(s), appropriate members of the affected departments and the IT staff will meet with legal counsel to identify the set of data that must be preserved and the persons responsible for ensuring its preservation.

4. The Vice President of Technology and members of the IT staff will meet with all affected individuals to identify potential locations of data related to the litigation and to create a plan to preserve all required data. The Vice President of Technology, in cooperation with legal counsel, will keep a record of the individuals contacted about data preservation, the instructions given to those individuals, and the steps taken to preserve the data.

5. IT will work with affected individuals to implement preservation of the data in its original electronic form. This may include, but will not be limited to, the following:

- Suspending automatic destruction of potentially discoverable data;
- Preserving snapshots of the NAS;
- Cloning the Banner database to a separate database to which only the Banner DBA and Banner System Administrator have access;
- Collecting a full system image of appropriate centrally-managed servers;
- After removal of personal data (e.g., personal tax documents, personal word documents, and personal e-mail, unless such personal information is relevant to the matter that triggered the litigation hold), collecting a full system image of appropriate individual computers; and
- Collecting copies of portable secondary storage.

6. IT will send specific instructions on handling information to all affected individuals to ensure that future data are preserved and easily retrievable.

7. IT will store all collected electronic data centrally for future potential retrieval and electronic discovery.