Records Management Policy

PURPOSE

Texas Wesleyan University is committed to effective records management. This policy is designed to:

- Safeguard the history of Texas Wesleyan University,
- Ensure adequate documentation in the event of litigation,
- Enhance compliance with applicable laws and regulations, and
- Facilitate the University's operations by promoting efficiency and freeing-up valuable storage space.

SCOPE

This policy applies to all University records, regardless of whether they are maintained in hard (paper) copy, electronically, or in some other fashion and all employees and vendors who manage University records.

POLICY

The University requires that its records and documents be managed in a systematic and logical manner, consistent with applicable laws. Each department handling University records shall develop and implement processes and procedures to meet the requirements outlined in this document.

Record and Document Retention
The University will retain records and documents in accordance with the University Record Retention Schedule. Records and documents not listed in the schedule that are substantially similar to those listed in the schedule, or that pertain to a particular transaction or matter documented by a record listed in the schedule, should be retained for the length of time required for the substantially similar/related record or document.

Record and Document Retention Schedule
The Record Retention Schedule is a control document that describes the records of the University by subject matter category, establishes a timetable for the maintenance, archiving or destruction of the records, prescribes an ultimate disposition for the records, and serves as the legal authorization for the disposition of records.

Electronic Records and Documents
Electronic documents will be retained as if they were paper documents. Therefore, any electronic file that falls into one of the document types on the schedule, or that represents a substantially similar/related document, will be maintained for the scheduled length of time.

E-mail messages and/or other electronic files that need to be retained under this policy should be either printed in hard copy and stored in the appropriate file or downloaded to a computer file and stored electronically or on a disk as a separate file. Email is not an approved location to store Confidential Personal Information nor Confidential Information. These email messages, whether encrypted or decrypted, must be immediately moved from the users' mailbox (inbox/sent items) to an appropriate, secure location.

Unencrypted email message may not contain any confidential data or confidential personal information. Any request to use encrypted email messages for communicating sensitive or protected information must be approved by the Information Security Manager.

Records and documents may not be stored or processed offsite (includes cloud-based providers) without prior approval from both the University's Record Retention Officer and Chief Information Officer. Only service providers who a) have been evaluated and approved by IT Infrastructure Services and b) meet all requirements identified in the University's Network Protection and Information Security Policy may be considered for use.

Business Continuity
University records will be stored in a safe, secure, and accessible manner. Documents and financial files that are essential to keeping the University operating in an emergency, are to be duplicated and backed-up on a regular schedule.

Record and Document Disposition
Departments are responsible for the safe and secure maintenance, storage, and disposition of their own records, with oversight by the Record Retention Officer's designee. The Business Office will serve as a resource for the ongoing process of identifying records that meet the required retention period.

The following hardcopy records will be destroyed by shredding:

- University financial records;
- Individually-identifiable financial, medical, student, or personnel-related records; and
- Any other documents or records containing Confidential Information or information of a sensitive nature.

Litigation Hold
Document disposition will be suspended immediately and all potentially relevant records and documents, whether listed on the Retention Schedule or not, must be preserved and maintained when a lawsuit is filed or is reasonably anticipated. Records and documents that are subject to a "litigation hold," as determined by the Vice President of Finance and Administration or Office of Human Resources, shall be preserved and retained until such time as the Vice President of Finance and Administration or Office of Human Resources specifically authorizes the disposal of the documents.

Records that are subject to a litigation hold shall not be destroyed in accordance with standard destruction procedures. As such, upon initiation of a litigation hold, these records must be immediately segregated from other records so they are protected from any routine record purges. This is especially critical for emails or other electronic documents that may be subject to a computerized purge cycle. Please see the vice president immediately if you have any questions about this procedure.

ROLES AND RESPONSIBILITIES

The Vice President of Finance and Administration is designated as the University's Record Retention Officer (RRO). The RRO shall, either directly or via the assignment of a designee, have responsibility for overseeing institutional compliance with this policy. The RRO shall be responsible for ensuring that each department, committees or other subset of the University conducts an annual audit to ensure that all University records are maintained in accordance with this policy. The RRO shall have the authority to require periodic third-party reviews of the University's record retention and destruction practices.

The RRO shall annually ensure that all departments and any vendors who use, maintain or store University records are complying with this policy, including the storage and destruction of Confidential Data and Confidential Personal Information. The RRO shall be responsible for reviewing applicable vendor contracts which involve use, maintenance or destruction of University records. The RRO shall ensure that these vendor contracts contain provisions that require compliance with this policy.

The Information Security Manager shall act as the designated Data Protection Officer and shall carry out all requisite activities associated with the General Data Protection Regulation (GDPR).

TERMS AND DEFINITIONS

Confidential Data - Confidential data should be protected as required by law and policy. Confidential data includes information that is protected as confidential by law, such as the Family Educational Rights and Privacy Act of 1974 (FERPA) (education records) or the Health Insurance Portability and Accountability Act's Privacy Regulations (HIPAA) (medical records) as well as any other information that the university, as a private entity, deems confidential and takes steps to protect. While the following is not intended as an exhaustive list, Confidential Data also includes the following categories:

- Any student, faculty or staff information made confidential or private by statute or regulation such as FERPA, HIPAA, GDPR, the American With Disabilities Act or the Family Medical Leave Act;
- Purchasing records prior to the opening of bids, or prior to the award of contracts resulting from requests for proposals;
- Trade Secret Proprietary information;
- Protected financial and contract information; and
- Information the university has contractually agreed not to disclose.

Confidential Personal Information (a.k.a. Personally Identifiable Information) – an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- Social Security Number;
- Driver license number or government-issued ID number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Confidential Personal Information also includes information that identifies an individual and relates to:

- The physical or mental health or condition of the individual;

- The provision of health care to the individual; or
- Payment for the provision of health care to the individual.

Confidential Personal Information does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

Records
Records are information fixed in any media and include, but are not limited, to the following formats: paper and electronic documents, audio and video recordings, databases, emails text messages and/or instant messages (collectively known as “Records”).

Unofficial Records
Unofficial Records are not subject to this policy. Unofficial records are:

- Private or personal documents that are not created or received in the course of the University's business;
- Extra Copies of Official Records. For example, for each official policy, there will be copies of this policy distributed to employees. Any copies are not Official Records.
- Faculty records created or received solely in the course of faculty research or professional activities, such as interview or survey results, databases, or manuscripts materials are not Official Records. Note that Records created or received by faculty in the course of teaching, advising, committee work, research administration or program, department or institution administration are Official Records under this policy.

Official Records
Official Records are Records that are created or received in the ordinary course of the University’s business. Official Records are the property of the University and must be maintained, preserved or destroyed in accordance with this policy.

Official Records, include, but are not limited to: correspondence; minutes; memos; drawings; maps; computer data; machine readable data; reports; newsletters; published materials; institutional policies and procedures; financial records, including invoices, journals, ledgers, purchase orders, grant documentation or other records pertaining to fiscal information; personnel records, including evaluations and other communications regarding an employee’s performance.

RELATED DOCUMENTS

Network Protection and Information Security Policy
Security Incident Reporting and Response Policy
University Record Retention Schedule