Records Management Policy

PURPOSE

Texas Wesleyan University (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. Non-records, as defined below, are not subject to this Policy and may be destroyed at any time.

This Policy applies to all University 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 shall develop and implement processes and procedures to meet the requirements outlined in this document. Each department shall designate a Records Management Liaison who will be responsible for coordinating the department's compliance with this Policy, including the maintenance of the department's Official Records, the destruction of University Records, and the management of Records in accordance with the University's Record Retention Schedule.

Record and Document Retention
The University will retain records and documents in accordance with the University's 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. The Record Retention Officer or its designee is responsible for maintaining the Record Retention Schedule. Questions regarding this Policy or the Record Retention Schedule should be directed to the Record Retention Officer or its designee. The Record Retention Schedule may be updated, changed, or amended as necessary. The Record Retention Officer, Chief Information Officer, or their designee may implement practices and procedures consistent with this Policy and the Record Retention Officer to ensure effective and efficient methods of records management.

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.

Records and documents may not be stored or processed offsite (includes cloud-based providers) without prior written approval from the University's Record Retention Officer or Chief Information Officer. Employees, for example, should not store or create Records on a Google drive that has not been disclosed or authorized by the 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 relevant technology policies 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 Record Retention Officer's designee will serve as a resource for the ongoing process of identifying Records that meet the required retention period and the appropriate manner of disposing of Records.

When a record includes Confidential Data, Confidential Personal Information, or privileged information, the Records must be destroyed or disposed of in a secure manner. The following hardcopy Records, for example, 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, Confidential Personal 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 Record 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, Office of Human Resources, or General Counsel shall be preserved and retained until such time as the Vice President of Finance and Administration, Office of Human Resources or General Counsel 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 of Finance and Administration 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. The Record Retention Officer shall, either directly or via the assignment of a designee, have responsibility for overseeing institutional compliance with this Policy. The Record Retention Officer 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 Record Retention Officer shall have the authority to require periodic third party reviews of the University's record retention and destruction practices.

The Record Retention Officer 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 Record Retention Officer shall be responsible for reviewing applicable vendor contracts that involve use, maintenance, or destruction of University Records. The Record Retention Officer shall ensure that these vendor contracts contain provisions that require compliance with this policy.

TERMS AND DEFINITIONS

Confidential Data - A sensitivity designation for information, the disclosure of which is expected to damage Texas Wesleyan or its partners; this includes information protected by statutes, regulations, University policies or contractual language.

Confidential Personal 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.

Non-Records - any document, device, or items that does not mean the definition of "Records." The following are unlikely to be considered Records:

- Private or personal documents that are not created or received in the course of the University's business;
- Non-university publications;
- Listserv materials;
- Junk mail/spam;
- Catalogs; and
- Faculty records created or received in the course of faculty research or professional activities. 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 Records under this Policy.

Official Records - Official Records are Records that are created or received in any format in the 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: archival records, financial aid records, personnel records, correspondence, minutes, memos, drawings, reports, institutional policies and procedures, financial and accounting records, legal documents, regulatory/compliance records, safety records, and grant and donor documentation.

Records – Information owned in part or whole by the University, that is fixed in any media and include but are not limited to the following formats: paper and electronic documents, audio and video recordings, databases, emails and/or text messages.

Approved by Texas Wesleyan University Executive Staff on October 31, 2022