Records Retention Policy

Document Number: BUSO-0020 **Date Published(sys):** 2/6/2024

General Description

Purpose:

The purpose of this Records Retention Policy (Policy) is to provide for the systematic review, retention, and disposition of documents and records received, created, or maintained by Trinity University (University) in connection with University business. This policy contains a schedule for how long certain documents should be retained and how they should be disposed of (unless they are under a legal or other similar investigation or are otherwise subject to a litigation hold).

The policy is designated to:

- Preserve the history of the University,
- Ensure adequate documentation in the event of litigation or an administrative agency charge,
- Comply with federal and state laws and regulations,
- Eliminate accidental or innocent destruction of records required to be retained, and
- Facilitate the University's operations by promoting efficiency and freeing-up valuable storage space.

Scope:

This policy applies to all employees who manage University Records. This policy also applies to all outside vendors or volunteers whose work or services for the University requires the management of University Records.

Exceptions:

None.

Policy Content

Record and Document Retention

The University will retain Records in accordance with the University Record Retention Schedule. All University employees and others subject to this policy must comply with this policy, the University Record Retention Schedule, and any litigation hold communications. Failure to do so may subject the University, its employees, and outside vendors to civil or criminal liability.

Note: No document list can be exhaustive. Questions regarding the retention period for any specific document or class of documents not included in the University Record Retention Schedule should be addressed to the Office of General Counsel (OGC).

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 authorization for the disposition of Records.

Records 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.

Electronic Records and Documents

Electronic records will be retained as if they were paper documents. Therefore, any electronic files that fall into one of the document types on the schedule or that represent a substantially similar/related document as discussed above, 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 (i) printed in hard copy and stored in the appropriate file or (ii) downloaded to a computer file and stored electronically or on a disk as a separate file.

This policy does not cover all situations or scenarios within the workforce of the campus community. It has been established to guide processes that outline and define Trinity's actions in handling email accounts, data, etc. It is understood and recognized that not all categories and events may be captured within this policy. In these instances, we will work with the authoritative department to work out flexible or other suitable arrangements as required. It is the authoritative department’s responsibility to request changes or modifications to this policy and Trinity University’s process and procedures for disabling and deleting accounts and user data. Additionally, it is the authoritative department’s responsibility to request access to a recently separated or terminated employee’s files in order to review and take appropriate action for the retention of documents, email correspondence and files.

Currently Enrolled or Employed

	Email Account	AD Account	User Date
Faculty (FT)	Active	Active	Active

Faculty (Non FT)	Active	Active	Active
Faculty (Emeritus)	Active	Active	Active
Staff (FT & PT)	Active	Active	Active
Students (FT & PT)	Active	Active	Active
Contractors/Vendors	Active	Active	Active

*Does not include legal holds or other University proceedings that require longer retention and preservation of data and files.

Upon Separation, Termination, Graduation, Inactivity, etc.
(DA = Disable) (DE = Delete)

	Email Account	AD Account	User Data
Faculty (FT)	(DA) Departure	(DA) Departure	(DE) After 45 Days
Faculty (Non FT)	(DA) Departure; (DA) 1 year after last course	(DA) Departure; (DA) 1 year after last course	(DE) After 45 Days
Faculty (Emeritus)	Active	Active	Active
Staff (FT & PT)	(DA) Departure	(DA) Departure	(DE) After 45 Days
Students	(DA) Upon Dismissal (DA) 1 year after Graduation (DA) 180 No Activity	(DA) Upon Dismissal (DA) Upon Departure (DA) 180 No Activity	(DE) 45 Days after dismissal, departure, graduation; or (DE) Same time after 180 inactivity period
Contractors/Vendors	(DA) Departure (DA) After 60 Days Inactivity	(DA) Departure (DA) After 60 Days inactivity	(DE) 180 days

Classification, maintenance, retention, archiving and/or disposal of electronic records is the responsibility of the e-mail user, depending on the category of the Electronic Record, and must be in accordance with guidelines established by the University and also in compliance with Record Retention Schedule. For example, if an email contains housing assignments, it would be considered a Housing Assignment Record and maintained permanently per the Retention schedule.

Failure to properly maintain electronic records may expose the University and individuals to legal risks. Work-related emails are University records, and must be treated as such. E-mail that does not meet the definition of University record, e.g., personal or junk email, should be deleted immediately from the system and not be commingled with work-related messages.

It is important to note that the e-mail message should be kept with the attachment(s). The printed copy of the e-mail must contain the following header information: (1) who sent the message, (2) whom the

message was sent to and (3) the date and time the message was sent, and (4) the subject of the message.

When an email is used as a transport mechanism for other types of records, it is possible, based on the content, for the retention and disposition period of the e-mail and transported record(s) to differ. In this case, the longest retention period shall apply.

The University servers are intended for short-term record retention. Information Technology (IT) performs backups on a regular schedule of the email and electronic files stored on central servers for disaster recovery. These backups are to be used for system restoration purposes only. IT administrators are not the legal custodians of messages or records which may be included in such backups. The disposition and retention of electronic records must be coordinated with the University's Information Technology Department.

It is the end user's responsibility to manage the proper maintenance, storage and handling of email messages and documents received via email. This management process includes following the Trinity University Retention Schedule as email is not a storage location for files, documents or official University business correspondence.

Disaster Planning and Preparedness

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 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 each vice president or their designee. The Office of Finance & Administration will serve as a resource for the ongoing process of identifying records that meet the required retention period. Once Records have been identified as having met the retention period, the following hardcopy Records will be destroyed by shredding: 1) University financial records; 2) individually-identifiable financial, medical, student, or personnel-related records; and 3) any other documents or records containing Confidential Information, as defined above, and/or non-public information about the University. If in doubt as to the proper method to destroy a document, shred it.

The disposition of electronic records must be coordinated with the University's Information Technology Department.

Litigation Hold

When litigation against the University or its employees is filed or threatened, the law imposes a duty upon the University to preserve all documents and records that pertain to the issues. As soon as the OGC is made aware of pending or threatened litigation, a litigation hold directive will be issued to the legal custodian. The litigation hold directive overrides any record retention schedule that may have otherwise called for the transfer, disposal, or destruction of the relevant documents until the OGC has cleared the hold.

If a litigation hold is placed with respect to certain documents, there is a legal duty to maintain these documents in their original form, and they should not be destroyed or altered until the lawsuit is resolved. The documents may be scanned into electronic form, but the original paper documents should not be destroyed after scanning and should be maintained for the pendency of the lawsuit. Once the litigation is resolved and the litigation hold is lifted, the paper documents may be shredded after the documents have been scanned.

Email and computer accounts of separated employees that have been placed on a litigation hold by University Counsel will be maintained by IT until the hold is released.

No employee whom University Counsel has notified of a litigation hold may alter or delete any record that falls within the scope of that hold.

Performance Evaluation

Consequences of Policy Violation:

All employees and others subject to this policy may be subject to punitive action for violations of this policy up to and including suspension or termination of employment, cancellation of contract, removal from the University, and/orpossible civil and criminal sanctions. Questions about the enforcement of this policy should be referred to the head of the department that possesses or maintains the records or the OGC.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Records or Documents	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 the “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

Term:	Definition:
	course of the University's business; • Extra Copies of Official Records. For example, for each official policy, copies of this policy will be 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 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 by this policy. Official Records include, but are not limited to: correspondence (including e-mails); 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 about fiscal information; personnel records, including evaluations and other communications regarding an employee's performance.
Personally Identifiable Information	Personally Identifiable Information (PII) under the Family Educational Rights and Privacy Act of 1974 (FERPA) is defined as identifiable information that is maintained in education records and includes direct identifiers, as well as indirect identifiers or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. PII includes but is not limited to: • A student's name; • The name of the student's parents or other family members; • The address of the student or the student's family; • Personal identifiers, including a student's social security number, student identification number, or biometric record; • Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; • Other information that alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant

Term:	Definition:
	circumstances to identify the student with reasonable certainty; or • Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. PII is highly sensitive and must be safeguarded and secured at all times in accordance with the provisions of FERPA and this policy.
Confidential Information	Confidential Information should be protected as required by law and policy. Confidential information includes information that is protected as confidential by law, such as FERPA (education records), GLBA, or the Health Insurance Portability and Accountability Act's Privacy Regulations (HIPAA) (medical records), as well as any other information that Trinity, as a private university, deems confidential and takes steps to protect as such. While the following is not intended as an all-inclusive list, Confidential Information also includes the following categories: • Any student, faculty, or staff information made confidential or private by statute or regulation such as FERPA, GLBA, HIPAA, the American With Disabilities Act, or the Family Medical Leave Act; • Personnel information; • Purchasing records before the opening of bids or prior to the award of contracts resulting from requests for proposals; • Trade Secret Proprietary information; • Financial and contact information; and • Information the University has contractually agreed not to disclose.

Related Documents

Related Content:

Record & Document Retention Schedule

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.5	12/1/2023 9:46 AM	Pamela Mota
v2.0	4/26/2023 8:36 AM	Holly Warfel
v1.0	7/25/2019 12:22 PM	Holly Warfel

Vice President Approval:

Name:	Title:
Gary Logan	Vice President for Finance & Administration