

KANSAS STATE UNIVERSITY FOUNDATION

Title	Document Retention and Destruction Policy	Version	7
Approved By	Kansas State University Foundation Board of Directors	Approval Date	09/26/2025
Approved By	Governance Committee	Approval Date	09/25/2025
Liaison to the Committee	Greg Lohrentz (Senior Vice President of Operations and Finance/COO/CFO)		

Printed copies are for reference only. Please refer to the electronic copy in PolicyTech for the latest version.

Rationale

Records are a vital resource of The Kansas State University Foundation (the “Foundation”) requiring prudent management. Records serve as evidence of the Foundation's organization, functions, policies, decisions, procedures, operations, or other activities. This Document Retention and Destruction Policy (this “Policy”) is established to ensure that the records (as defined below) of the Foundation are retained as required by law, and/or for a period deemed to be sufficient given the content and purpose of the record, and that unnecessary information is appropriately destroyed following the applicable retention period..

Applies to

This Policy applies to all officers, directors and employees and any other person who has access to the Foundation’s records.

Policy

A. Reasons for Policy

The Foundation must retain certain records because they contain information that:

- Serves as the Foundation's corporate memory.
- Have enduring business value (for example, they provide a record of a business transaction, evidence the Foundation's rights or obligations, protect the Foundation's legal interests or ensure operational continuity).
- Must be kept to satisfy legal, accounting, or other regulatory requirements.

The Foundation prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information. The accidental or intentional destruction of records ahead of their specified retention periods could result in the following consequences for the Foundation and/or its employees:

- Fines and penalties.
- Loss of rights.

- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

Maintenance of records beyond the applicable retention period results in increased storage costs, physical and electronic clutter, and inefficiency.

B. Types of Documents

This Policy explains the differences among “records”, disposable information, and confidential information belonging to others.

Records. For purposes of this Policy a “record” is any type of information (other than “disposable information” as defined below) created, received, or transmitted in the transaction of the Foundation’s business, regardless of physical format. Examples records and where they may be located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs.
- Contracts.
- Electronic files.
- Emails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Memory in cell phones, tablets, and similar devices.
- Voicemails.

The Foundation and its employees must retain records for the period indicated in the [Record Retention Schedule](#) attached to this Policy and must be retained for the amount of time indicated in the Records Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If a record does not fall within a category on the Record Retention Schedule, it should be destroyed as soon as it no longer serves a useful business purpose. The Foundation presumes that categories of records that are not listed on the Record Retention Schedule will have a useful business purpose for no more than 7 years after their creation or subsequent modification, and that such records should be destroyed after that period (or earlier). If you are unsure whether to retain a certain Record, contact the Records Management Officer (as defined in part F below). The Records Management Officer or COO may determine that a category of records not listed on the Record Retention Schedule should be retained for more or less than 7 years.

It is important to note that emails may have a different retention period than a record that is attached to an email. This Policy requires employees to save records attached to emails outside of an email software program or server (such as Microsoft Outlook or Gmail). If the email is integral to understanding the attached record, it should be saved along with the record outside of the email software program. If an email no longer serves a business

purpose, it may be deleted from the email software program.

Disposable Information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this Policy.

Examples may include:

- Convenience materials, such as notes or annotated copies of documents, created by staff for their own use and which have short-term referential value and no historical significance or long-term business importance
- Duplicates of originals.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Foundation and retained primarily for reference purposes.
- Spam and junk mail.
- Emails or other communications that no longer serve a business purpose

Confidential Information Belonging to Others. Any confidential information that an employee may have obtained from a source outside of the Foundation, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by the Foundation. Unsolicited confidential information submitted to the Foundation should be refused, returned to the sender where possible, and destroyed or deleted.

Additionally, agreements with third parties, such as confidentiality and non-disclosure agreements, may require specific rules for destruction or retention of a third-party's information. It is important that these contractual obligations are followed, notwithstanding this Policy.

C. Mandatory Compliance

Responsibility of All Employees. The Foundation strives to comply with the laws, rules, and regulations that govern it and with recognized compliance practices. All Foundation employees must comply with this Policy, the [Record Retention Schedule](#) and any litigation hold communications.

Failure to do so may subject the Foundation, its employees, and contract staff to serious civil and/or criminal liability. An employee's failure to comply with this Policy may result in disciplinary sanctions, including suspension or termination.

Reporting Policy Violations. The Foundation is committed to enforcing this Policy as it applies to all forms of records. The effectiveness of the Foundation's efforts, however, depends largely on employees. If you feel that you or someone else may have violated this Policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the Records Management Officer. If employees do not report inappropriate conduct, the Foundation may not become aware of a possible violation of this Policy and may not be able to take

appropriate corrective action. No one will be subject to and the Foundation prohibits, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind relating to this Policy or cooperating in related investigations.

D. How to Store and Destroy Records

Storage. The Foundation's records must be stored in a safe, secure, and accessible manner. Electronic Records should be stored as instructed by the IT Department which shall develop and abide by appropriate data security policies including a requirement that person with access to confidential or sensitive information owned or used by the Foundation shall sign and abide by an annual confidentiality statement

Destruction. The Foundation's records Management Officer is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of physical confidential, financial, and personnel-related records must be conducted by shredding if possible. Non-confidential records may be destroyed by recycling. The destruction of electronic records must be coordinated by the IT Department.

The destruction of records must stop immediately upon notification that a litigation hold is to begin because the Foundation may be involved in a lawsuit or an official investigation (see next paragraph). Destruction may begin again once the COO lifts the relevant litigation hold.

E. Litigation Holds and Other Special Situations

The Foundation requires all employees to comply fully with its published [Record Retention Schedule](#) and procedures as provided in this Policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or a manager or outside legal counsel informs you, that the Foundation Records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until outside legal counsel determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold, and it replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply or have any questions regarding whether it may possibly apply, please contact the COO.

In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the replacement of the Foundation's information technology systems.

F. Records Management Officer

The Records Management Officer is responsible for identifying the documents that the Foundation must or should retain, and determining, in collaboration with outside legal counsel, the proper period of retention. He or she also arranges for the proper storage and

retrieval of records, coordinating with outside vendors where appropriate. Additionally, the Records Management Officer ensures the destruction of records whose retention period has expired.

The Foundation has designated Katy Walradt as the Records Management Officer. The Records Management Officer's contact information is: katyw@ksufoundation.org or 785-775-2117. The Records Management Officer is responsible for:

- Administering and monitoring compliance with the Foundation's document management program and helping department heads and employees implement it and related best practices.
- Establish and implement this Policy and best practices for appropriate preservation and disposal of the Foundation's records.
- Coordinating with the COO and IT to ensure that only appropriate authorized users have access to nonpublic records.
- In cooperation with department heads, identifying essential Records and establishing a disaster plan for each office and department to ensure maximum availability of the Foundation's Records to reestablish operations quickly and with minimal interruption and expense.
- Periodically conferring with outside counsel to review the [Record Retention Schedule](#), which references to applicable law.
- Informing employees of their duties relating to document management.
- Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from departmental staff.
- Evaluating the overall effectiveness of the document management program.
- Reporting annually to the COO on the implementation of the document management program in each of the Foundation's departments.
- Bringing to the attention of the COO any noncompliance by department heads or other employees with this Policy and the Foundation's document management program.

G. Audits and Employee Questions

Internal Review and Policy Audits

The COO of the Foundation and the Records Management Officer will periodically review this Policy and its procedures with outside legal counsel and/or the Foundation's certified public accountant to ensure the Foundation is in full compliance with relevant new or amended regulations. Additionally, the Foundation will regularly audit employee files and computer hard drives and other relevant forms of storage to ensure compliance with this Policy.

Questions about this Policy

Any questions about this Policy should be referred to the Records Management Officer, who oversees administering, enforcing, and updating this, Policy.

Definitions

There are no definitions for this policy.

Procedures

There are no procedures for this policy.

References & Links

[Record Retention Schedule](#)

Contact

Department Name or Person	Phone Number
Sr VP of Operations and Finance/COO/CFO	785-775-2010
AVP of Investments	785-775-2127
AVP of Talent, Culture & Human Resources	785-775-2012
VP of Marketing Communications	785-775-2016
AVP of Information, Technology and Infrastructure	785-775-2236
AVP of Accounting/Controller	785-775-2102
Director of Compliance	785-775-2117