Header

Policy Name and Number: **L1.1 Records Retention**

Policy Developer(s): Office of Legal Affairs

Original Date: May 13, 2021

Last Review Date: NA

Approval Date: May 13, 2021

Contact Person for Website: University Counsel

Body

POLICY

John Carroll University ("the University") requires that certain types of University records be retained for specific periods of time in accordance with legal and institutional requirements. These records can be destroyed after these retention periods have ended. The University has designated Offices of Record or Data Stewards to manage the retention and disposal of such records in accordance with this policy.

PURPOSE

The University is committed to effective records retention and destruction to preserve its history, comply with legal requirements, optimize the use of space, minimize the cost of record retention, reduce exposure to cyber-security incidents, and ensure that outdated and unnecessary records are disposed of or destroyed.

SCOPE

This policy pertains to all employees of John Carroll University. It applies to all records regardless of format or storage method or location, including all paper, electronic, microform and all other formats.

PROCEDURES

A. Retention and Destruction of Records

1. Retention Schedules

a. University records must be retained for the amount of time prescribed in the Retention Schedules located at https://jcu.edu/university-committees/university-policies-and-data-retention-schedules#sched. The Office of Record shall determine the appropriate retention period for records in that particular department or division. These retention periods shall be documented in a Retention Schedule for that department or division. The Office of Record must consider institutional needs, accreditation needs, historical needs, and other legal and administrative factors in developing their Retention Schedule.

b. Retention Schedules must be approved by the appropriate divisional Vice President and then submitted to the Data Governance Committee for endorsement. Each Retention Schedule will then be forwarded to the Office of the Provost and Academic Vice President and Vice President for Finance and Administration for final approval and posting for the University community. Questions regarding content of Retention Schedules should be directed to the Office of Legal Affairs, who will consult with the Office of the Provost and Academic Vice President or the Vice President of Finance and Administration regarding such questions. The Provost and Academic Vice President, Vice President for Finance and Administration, or the Office of Legal Affairs may determine and approve that a given type of record should be retained for a different period than the Retention Schedule requires.

c. Once the recommended retention period is submitted and posted, the Retention Schedule will be implemented by the Office of Record.

d. The Data Steward for each Office of Record must educate its respective faculty and/or staff within the department or division regarding this policy and Retention Schedule(s), and must enforce the provisions of this policy and the Retention Schedule(s).

e. Departments that are not Offices of Record of certain records but which possess copies of such records are not responsible for retaining the records for the retention period and should dispose of the records when the records are no longer in active use by the non-official department. Such departments should confirm that the Office of Record does, in fact, possess the original record prior to its destruction.

f. Retention periods may change from time to time due to changes in the law, audit requirements or other factors. Any such changes supersede the requirements listed in the Retention Schedule, and the Retention Schedule(s) will be updated to reflect this change.

2. **Record Destruction**: When the required retention period for a record has passed, the record should be responsibly destroyed as described below. The Retention Schedule will describe whether or not such destruction is mandatory.

   a. *Paper Records*: Paper records should be either (a) discarded, preferably in recycle bins, if the records do not contain Confidential Information or Sensitive Data or (b) securely shredded if the records contain ANY Confidential Information or Sensitive Data. Information regarding obtaining shredding services is available from the University Mail Room.

   b. *Electronic Records*: Electronic records must be destroyed in the manner prescribed by the University's Chief Information Officer and consistent with the Sensitive Data & Security Policy.

   c. Faculty members who serve in both faculty and administrative roles (e.g., deans, chairs, department heads and directors) may destroy outdated and unnecessary records relating solely to their faculty role (e.g., research records and teaching materials) in accordance with this policy, unless otherwise prohibited by law or policy. These individuals should destroy

records relating to their administrative functions (e.g., personnel records, student records and department operations records) in accordance with this policy.

d. All other University personnel should destroy records in accordance with this policy.

B. Electronic Records

1. This policy applies equally to records that exist in electronic (including email) or paper form. It is the content and function, not the form, of any record that determines its retention period.
2. Users must retain or dispose of electronic records according to the retention periods in the applicable Retention Schedule, just as they would for paper records.
3. Information Technology Services (ITS) maintains electronic backup copies of certain University data to provide a means for recovery of data that has been inadvertently deleted. These backup copies are retained and destroyed on schedules created to match the specific Retention Schedule described above.
4. All data associated with Google Suite applications, including any automatic backup copies, are retained by Google indefinitely unless deleted by the user. Deleted data may be recoverable as provided for by Google at the time of deletion. The University has no control over the retention parameters of this functionality.
5. The Chief Information Officer will determine appropriate protocols for the disposal of electronic records.

C. Archival Records

1. An archival record is a record that has permanent institutional or historical value to the University.
2. Archival records are retained and preserved indefinitely in the University's Library Archives or the Office of Record.
3. The Retention Schedules for archival records indicate "indefinite" as the required retention period.
4. The University Library Archives has developed a Records Retention Policy for the Archives. The Office of Record should consult with the Library Archives Records Retention Policy regarding the use and indefinite storage of materials in the Archives. Each Office of Record determines whether it believes a record should be classified as an archival record. The Office of Record should consult with the Library Archives and the Office of Legal Affairs to determine whether records can or should be submitted to the University Archives.
5. When an archival record is no longer in active use by the Office of Record, the archival record should be designated for indefinite retention and preservation.

D. Suspension of Record Destruction

1. Destruction or disposal of certain records pursuant to this policy must be immediately suspended whenever the University is involved in litigation, reasonably anticipates litigation or is the subject of a subpoena, government audit, investigation or Office of Legal Affairs "litigation hold" to which such records may apply. Once the University has notice of or reasonably anticipates litigation, a subpoena or government audit or investigation, the University must preserve all documents and records (in all formats) that relate to the matter.
2. Destruction or disposal of any record, in whatever form, that relates to pending or threatened litigation or government investigation, or that relates to any matter about which litigation or investigation is reasonably foreseeable, or that is the subject of an Office of Legal Affairs "litigation hold" (i.e., a communication from the Office of Legal Affairs advising not to destroy any records relating to a particular matter) directive, is strictly prohibited by this policy.
3. Departments must immediately notify the Office of Legal Affairs upon receipt of notice or reasonable anticipation of any litigation, subpoena, audit or investigation. The Office of Legal Affairs will instruct individuals likely to have relevant records to preserve such records until further notice from the Office of Legal Affairs and implement litigation hold practices to preserve the records. A preservation notice from the Office of Legal Affairs (i.e., a litigation hold) supersedes the Retention Schedules.

DEFINITIONS

A. **Record**: Any papers, documents, books, photographs, tapes, films, sound and/or video recordings, computerized information or other material, regardless of physical form or characteristics or storage method, made, produced, received or executed by any department or office of the University or by any academic or administrative personnel in connection with the performance of University business. Records also include databases and other data compilations.

   For purposes of this policy, records do not include: miscellaneous or personal papers or correspondence done outside the scope of employment or without official significance; extra copies of documents preserved only for convenience of reference; versions or drafts of reports, memos, files, superseded printed drafts and other such documents used to develop a final official record.

B. **Official Record:** Either (a) a record that has legally recognized and enforceable qualities that establish a fact, policy, institutional position or decision, or (b) a single official copy of a document maintained by a division or department, typically the original.
C. **Data Steward:** A University employee with delegated oversight and decision-making responsibility for a subset of the University's data. They have significant technical expertise in data under their purview and deep knowledge of related business processes. They may supervise or also serve as functional data technicians in the day-to-day capture and maintenance of specific subsets of data in related transactional databases.
D. **Office of Record:** The department or division designated as having responsibility for retention and timely disposal or destruction of particular types of records. Such

responsibility is assigned to the department's or division's head or a designee. Offices of Record are named in the Retention Schedules located at add link when published.

E. **Confidential Information**: Material that the University is legally, contractually or otherwise obligated to keep confidential; information that could be used to the detriment of the University or individuals if read by, or otherwise communicated to, others; and other such sensitive information. By way of illustration, some examples of Confidential Information include: personally identifiable information such as social security numbers; student educational records and other non-public student data; personnel and/or payroll records; bank account numbers and other personal financial information; intellectual property (as broadly defined by the University); and information related to litigation.

F. **Sensitive Data**: Data designated as private or confidential by law or by the University. Sensitive Data includes, but is not limited to, employment records, medical records, student education records, personal financial records (or other sensitive personally identifiable information), protected research Data, trade secrets, classified government information, proprietary information of the University, or any Data that could harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally.

   Examples of Sensitive Data include JCU ID numbers; protected health information; financial data; educational records; intellectual property records; protected research records; donor profiles; or any information that could result in a material risk of identity theft, a violation of the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the Gramm-Leach-Bliley Act (GLBA), or otherwise harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally. Sensitive Data shall not include records that by law must be made available to the general public.

CROSS REFERENCES

University Policies including but limited to

1. Sensitive Data & Security Policy
2. Library Archives Records Retention Policy
3. Procedures for Sensitive Data Destruction

This policy will next be reviewed ***five years*** from the approval date/date of last review.