The University of Vermont

OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

Title: Records Management and Retention

Policy Statement

It is the policy of the university to protect the security, integrity and accessibility of records created or maintained in the course of institutional operations, to retain records in accordance with applicable laws and regulations, and to ensure that records that are no longer needed or of no value are discarded at the appropriate time.

Reason for the Policy

This policy is designed to create a compliance standard for university personnel with respect to the retention of records ("records") created or maintained in the course of institutional business, governing records from their creation or receipt to their final disposition. It is also intended to facilitate appropriate access to records, preserve records confidentiality as applicable, reduce the cost of records maintenance, retain institutional records insofar as required or desirable, provide documentation in the event of litigation, and ensure the orderly destruction of records as appropriate.

Applicability of the Policy

This Policy applies to all members of the university community who have access to university records, including, without limitation, individuals who are faculty, staff, students, contractors, consultants, temporary employees, volunteers, and affiliates of the university.

Definitions

Archival Records:	are permanent records that have historical or enduring value to the university.
Electronic Records:	are records maintained in a format that requires the use of technology to access. Electronic records may take many forms including, without limitation, e-mail, text messaging, voicemail, IM, word processing documents, spreadsheets, web content, databases, scanned images.
Records:	means any and all written or recorded information produced or acquired in the course of university business, including without limitation all papers, documents, e-mail messages, machine-readable materials, and any other written or recorded materials, regardless of their physical form or characteristics. See the "Special Consideration" section for more specific information on certain types of records.
Records Coordinator:	refers to the individual that has been assigned responsibility in each unit for overseeing that unit's records life cycle management.

Record preservation directive or litigation hold: is a formal notice issued by the Office of the General Counsel (OGC) or other senior-level administrator to notify university employees that the university is under a legal obligation to preserve potentially relevant information.

Record Retention Schedule (Retention Schedule): means the schedule that identifies specific university records for which a retention period has been specified. The retention periods are based on law or regulation, legal or contractual requirements, or set at the discretion of management.

Responsible Office: is the office identified on the Retention Schedule as responsible for the specific record(s) described.

Procedures

Departmental Responsibilities for Retention of Records

Records Schedule

The university's Retention Schedule identifies specific records that should be retained for business purposes inclusive of teaching and research, as well as those records retained to comply with applicable laws and regulations. The Retention Schedule identifies the Responsible Offices and the applicable retention period for each of these records. Responsible Offices are responsible to identify records they create or obtain that must be retained to support business or regulatory needs and ensure that the Records Schedule accurately reflects these requirements. Each department should designate a Records Coordinator with responsibility for ensuring that records are managed in accordance with this policy and the Record Management Guidelines. Inquiries regarding records retention and disposition including requests by responsible offices to amend the Retention Schedule should be directed to the Chief Privacy Officer.

Records shall be maintained in formats to support operational needs and that will meet Federal, State or Local regulatory requirements. Responsible Offices shall ensure that records may be produced in response to an audit, inquiry, or legal action.

Questions regarding access to, or provision of copies of, university records are governed by the university Records and Documents Requests Policy and should be directed to the Office of the General Counsel. Records may be shared within the university for legitimate operational purposes.

Records not Listed on the Records Schedule

Not all records that are created in the course of university operations are required to be retained. Those that are legally required to be retained should be listed on the Records Schedule. Other records maintained by departments for their internal use, convenience, and to facilitate their own operational needs may not be included in the Retention Schedule but may still be retained by departments to the extent that they facilitate operational needs. The Records Management Guidelines can provide assistance to departments in managing these records in accordance with this policy and sound records management practices. In addition to unique departmental records, these records may include copies of the records identified in the Retention Schedule that are kept by departments for convenience and efficiency. University offices that are not the Responsible Office are encouraged to limit the use, and retention, of redundant copies of records otherwise maintained by the Responsible Office.

Protection of Records Containing Protected University Information

All departments are responsible for the security and integrity of records that contain confidential or sensitive information. Records containing non-public protected data, or NPPD, as defined by the Privacy policy shall be maintained and secured in accordance with both the Information Security policy and the Privacy policy. Additionally, records containing NPPD that may personally identify an individual should be retained in a manner that protects and restricts transfer of the information to unauthorized persons and permits sharing information within the university on a "need-to-know" basis. Care must be taken when making copies of records containing NPPD to ensure the copy is assured the same level of security as the original and the information within the copy is shared in accordance with the university's Privacy policy.

Agreements with third party providers to retain university records should include the same standards for security, availability and integrity that are required of the responsible office; any agreements for storage of records containing NPPD require prior review by the Chief Privacy Officer (CPO) and General Counsel. Agreements for storage of electronic records containing NPPD by an external service provider require approval by the Information Security Officer (ISO) in consultation with the CPO and General Counsel as needed.

Incidents involving suspected security breaches of protected personal data must be reported in accordance with the university's Data Breach Notification policy.

Special Considerations

Archival Records

The university keeps Archival Records permanently. Most records covered by the records retention policy do not meet the criteria to be archived. In general, records have enduring value if they document the university's organizational structure and changes, history, strategic decisions, and social history, or are official publications. Archival records may include correspondence, reports, memoranda and notes, announcements, accreditation files, photographs, and meeting minutes. The University Archivist should be consulted when disposing records that may meet these criteria; no active records should be considered for archiving.

Electronic Records

Electronic records may be maintained in an electronic form that permits reasonable retrieval and access for the length of the prescribed retention period. Electronic record systems may require additional planning and maintenance to ensure that the systems and technology used to create, maintain, access, retrieve and dispose of the records remains functional throughout the length of the record's retention period. Electronic records management must include consideration regarding the ability to dispose of records at the end of their retention period. Additional considerations for electronic record systems include identifying security measures to ensure that the records maintained are accurate, authentic, free from unauthorized access or alterations and that disaster recovery plans exist.

Email

Email is one example of a record that is in an electronic format. Retention requirements for email will follow the university Records Retention Schedule only in circumstances where email is the format being used for the record described on the schedule. If an email record is recorded in an electronic or paper format outside of the university email system, and that other format will be considered the "master" record by the responsible office, there is no requirement to maintain the original email in the active email folder. Email records that are not records identified on the retention schedule shall be retained at employees' discretion and deleted when they no longer serve an administrative purpose. University

employees are responsible to retain and dispose of email that they send and receive in carrying out their employment responsibilities. Certain security precautions should be considered when using email for records retention, including (1) when sharing email records containing NPPD, restrictions on distribution should accompany the communication, and (2) unencrypted email shall not be used to exchange records containing NPPD.

Research Data

Principal Investigators (PI) are responsible for data collection, maintenance, and retention of university-owned Research Data in accordance with the sponsor's award agreement when applicable. The Records Retention Schedule identifies minimum retention periods for sponsored research data.

Record Preservation Directives (Litigation Holds)

In certain circumstances a record preservation directive or litigation hold notice may be issued in accordance with procedures established by the Office of General Counsel. Refer to the Record Preservation Directive UOP for more information. All involved staff and faculty must consult with the Office of General Counsel for direction relative to the preservation of relevant records.

No employee who has been formally notified of a record preservation directive may discard, destroy, alter, or delete a record that falls within the scope of that directive. Violation of the directive may subject the individual to disciplinary action, up to and including dismissal, as well as personal liability for civil or criminal sanctions by courts or law enforcement agencies.

Disposal and Destruction of Records

Unless prohibited from doing so for legal purposes (see Duty to Preserve Records), records should be disposed of as follows:

Records included in the Retention Schedule

Responsible university departments shall destroy records at the end of the records' retention period as prescribed by the Retention Schedule. Copies of records that are made by the Responsible Offices for their own convenience purposes should be destroyed no later than and in the same manner as the "master" records.

Records not included in the Retention Schedule

These records may be destroyed when they are no longer needed for business or operational purposes.

Any records containing NPPD as defined by the Privacy policy must be destroyed in a manner consistent with that policy to protect against unauthorized release of confidential information.

The University Archivist should be consulted when disposing of records that may meet the criteria for archival records.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	**Contact Information:**
Chief Privacy Officer	privacy@uvm.edu
Information Security Officer	iso@uvm.edu
University Archivist	uvmsc@uvm.edu

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- Data Breach Notification Policy
- Information Security Policy
- Privacy Policy
- Record Preservation Directives ("Litigation Holds") Operating Procedure
- Records and Documents Requests Policy
- Records Management Guidelines
- Records Retention Schedule

Regulatory References/Citations

- None

Training/Education

Training will be provided on an as-needed basis as determined by the Approval Authority or the Responsible Official.

About this Policy

Responsible Official:	Chief Privacy Officer	**Approval Authority:**	President
Policy Number:	V. 9.3.3	**Effective Date:**	March 18, 2018
Revision History:	• V. 9.0.3.1 effective November 9, 2007 • V. 9.3.2/V. 9.0.3.2 effective November 30, 2012 • V. 9.3.3 effective March 18, 2018. Minor revision September 30, 2021.		