Office of Audit, Compliance & Privacy Services

Records Retention:

To Keep or Not To Keep

Office of Privacy Services

privacy@uvm.edu

University of Vermont

Overview

- Why is Records Management Important?
- Who is Responsible for Records Management?
- What is a “Record?”
- Sources of Rules and about Preservation and Destruction
- Review of Policy, Schedule and Guidelines
- Common Records In Units
- Duty to Secure Sensitive Information
- Duty to Destroy
- Privacy Program & Records Retention Intersect
- Special Considerations
- Conclusion

Why is Records Management Important?

- Records are an information asset and hold value for UVM
- UVM has a duty to stakeholders to manage records effectively
- UVM must comply with regulatory retention requirements
- Some records contain protected, proprietary or sensitive information that must be safeguarded… some by regulation, some because it's the right thing to do.

Who is Responsible for Records Management?

Who is Responsible for Records Management?

- Every employee that creates, accesses, uses or discloses University records plays an important role in records management.
- Every employee has a responsibility to only create that which is necessary and part of their job duties.
- Every employee has a responsibility to only access, use or disclose records in accordance with UVM policy and within the scope of their job duties.
- Every employee has a responsibility to dispose of records for which they are responsible in accordance with University policy.
- Each employee needs to know the policy and know how to access the records retention schedule… or where to go for help when a record isn't listed.

What is a Record?

- Records are the evidence of what an organization does.
- Records capture the business activities and transactions, correspondence, student files, employee files, financial records, so on and so forth.
- Under VT law, most records are “public” records but not all records are “official” or need to be preserved.

What is a Record?

- Records are electronic, paper, video and recorded.
- Records can be in email, portable devices such as smartphones, portable storage such as external hard drives and thumb drives, laptops, desktops, servers.
- Records can be in file cabinets, storage boxes, third party storage facilities, campus facilities - attics and basements.

What is a Record?

- According to UVM Policy:

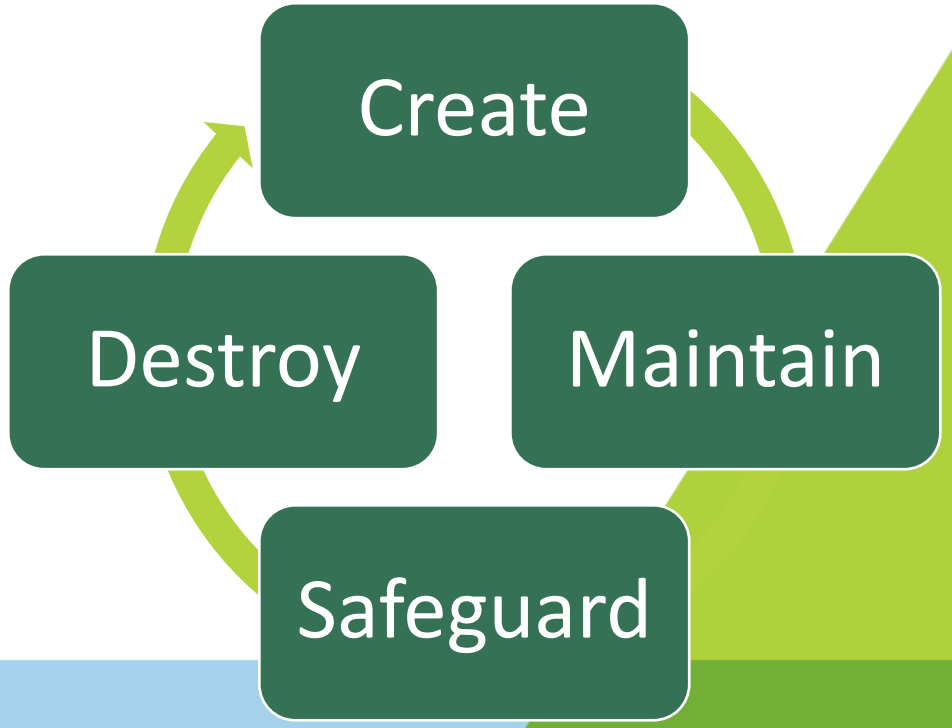
Records means any and all written or recorded information produced or acquired in the course of University business, including without limitation all papers, documents, e-mail messages, machine-readable materials, and any other written or recorded matters, regardless of their physical form or characteristics.

Sources of Rules about Preservation and Destruction

- Rules imposed upon us by law or other authority.
  - Vermont state laws, federal and international laws.
- Rules UVM fashions and imposes on ourselves.
  - UVM Policies, UOPs, Guidelines
- Whether a regulatory requirement or an institutional requirement, all employees are required to comply.

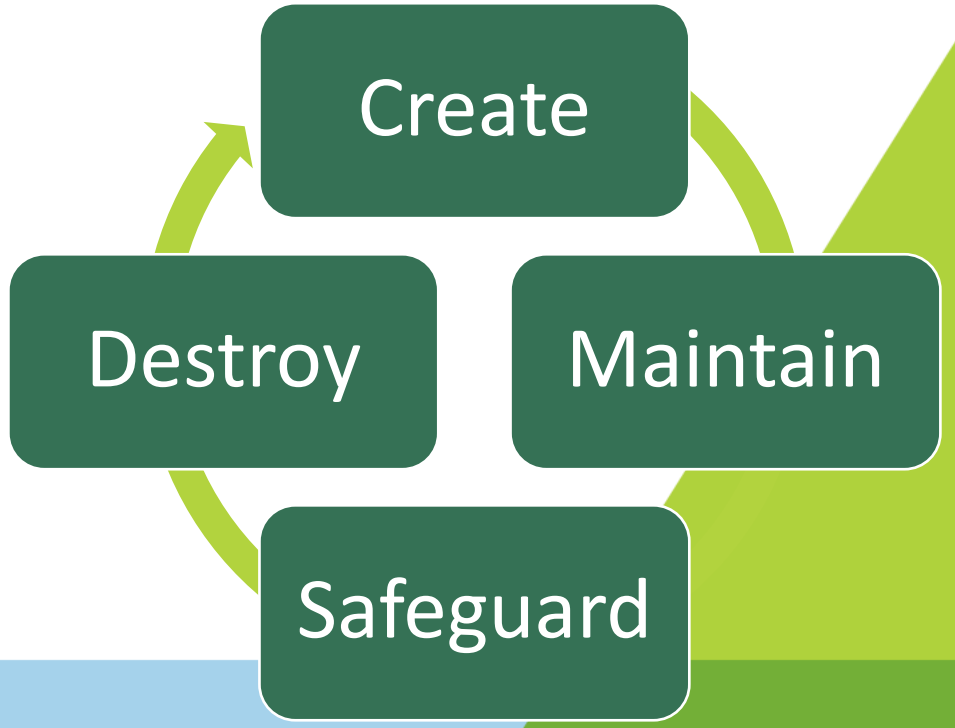
Review of Policy, Schedule and Guidelines

- UVM Records Retention Policy: https://uvm.edu/policies/records-management-and-retention
- ”Four Bucket” policy statement:
    1. Create
    2. Maintain
    3. Safeguard
    4. Destroy



Review of Policy, Schedule and Guidelines

- Create – once it's created, it's a record.
- Maintain – once a record has been created in the course of University business, we have an obligation to maintain it.



Review of Policy, Schedule and Guidelines

- Safeguard – protect and otherwise secure sensitive, protected, non-public personal, confidential or proprietary information contained in University records.
- Destroy – ensure that records that are no longer needed or have no value are discarded/destroyed at the appropriate time.

Review of Policy, Schedule and Guidelines

- UVM's Record Retention Schedule sets forth retention periods for University Records.
    - https://uvm.edu/compliance/compliance/public-records/record-retention-schedule
- We determine retention periods based on federal or state regulatory requirements, professional association guidance and management/operational needs.
- Schedule is updated as requirements change so always look to the online version for the most up to date.

Review of Policy, Schedule and Guidelines

- Terminology For Retention Periods Listed on Schedule:
  - ACT = Active, employed or enrolled
  - LIFE = Life of the record
  - AFYE = After fiscal year end
  - Other self-explanatory listings:
    - # Years
    - Permanent
    - Lifetime of License
    - Etc…….

Review of Policy, Schedule and Guidelines

- UVM developed guidelines to help units make decisions for records not listed in the schedule.
  - https://www.uvm.edu/sites/default/files/media/recordretention_guidlines_0.pdf
- RESPONSIBILITIES:
  - Chief Privacy Officer Responsible for policy and providing guidance.
  - Archivist Responsible for managing archives and identifying records to be preserved.
  - Individual unit leaders responsible for the records management for their units and assigning a Records Coordinator.

Review of Policy, Schedule and Guidelines

- Records Coordinators responsible for:
  - Identification and awareness of unit records
  - Managing the records lifecycle (creation, maintenance, disposition) of unit records
  - Knowledge of retention requirements listed on schedule
  - Creation of a schedule/program for unit records as needed
  - Familiarity with recordkeeping practices and standards in the guidelines

Common Records Under Unit Responsibility

- Common unit-level records:
  - Employment files not otherwise transferred to Human Resources;
  - Conflict of Interest Disclosure Forms and Conflict Management Plans (for non-officers)
  - Timesheets and supporting documentation (not otherwise kept in PeopleSoft or Kronos)
  - Employment Applications, Interview Notes, Reference Notes
  - Contracts
  - Financial Records and Backup Documentation
  - Training & Education Records, Certification & Licensure Records
  - Research Data
  - Email

Duty to Secure Sensitive Information

- Records containing protected personal data or sensitive university information require additional measures to safeguard the info from unauthorized disclosure.
- Unauthorized disclosure, depending on the information disclosed, may impose further reporting obligations as well as put those whose information has been compromised at risk.
- Increased federal, state and now international laws that impose heavy fines and penalties for breaches. Increased regulatory enforcement.

Duty to Secure Sensitive Information

- Records containing personal information must be secured (physical, administrative, technical) to prevent unauthorized disclosure.
- Accidental public disclosure of personal information requires reporting and disclosure in accordance with state, federal and international laws.
- More requirements for information such as social security numbers, credit card/bank/financial account numbers, driver's license numbers, health records, student record data.

Duty to Secure Sensitive Information

- FERPA: Protects Student Record Data
- HIPAA: Protects Protected Health Information (PHI) – Covered Components
- GLBA: Protects Non-Public Personal Information (NPPI) – Covered Areas
- GDPR: Protects Personal Data on EU Data Subjects – All areas that collect/process covered data
- Genetic Information Nondiscrimination Act (GINA)

Duty to Secure Sensitive Information

- Vermont Protection of Personal Information (62V.S.A. § 2430)
- Vermont Library Patron Records Act (22 VSA 171 et. seq.)
- Vermont Disclosure of Information Statute (18 V.S.A.§ 7103)
- Vermont Security Breach Notice Act (9 V.S.A. § 2435)
- Vermont Document Safe Destruction Act (9 V.S.A. § 2445)

Duty to Secure Sensitive Information

- Suspected privacy violations can be reported using the HelpLine or reported to the Chief Privacy Officer (privacy@uvm.edu) or the Information Security Officer (iso@uvm.edu)

Duty to Destroy

- When records have reached the end of their retention period, they should be discarded (if it's not personal, confidential, sensitive or protected) or destroyed (if it is.)
- Destroy does not mean just discard. Destroy means shred, Erase, or otherwise make it unreadable or indecipherable.
- Risks of keeping records longer than necessary:
    - Storage costs
    - Potential legal discovery during legal proceedings or regulatory audits/investigations
        - Once it's begun, relevant records can not be destroyed even if the retention period has been exceeded

Duty to Destroy

- UVM has a preferred pricing agreement for paper and tape destruction:
  - SecureShred, aka Shred This!
  - https://www.uvm.edu/finance/supplier-contracts-agreements
- Special consideration for computers, laptops and other technology… CD's, DVD's, thumb/flash drives, smartphones, tablets, other personal devices.
  - Resources:
    - https://www.uvm.edu/it/kb/article/secure-erase/
- Part of UVM's information security and privacy program.

Privacy Program and Records Retention Intersect

- Think about your needs before collection.
- If you don’t need it, don’t collect it.
- If you don’t collect it, you can’t lose it, it can’t be breached, there can’t be unauthorized access or inappropriate disclosure.
- If you need it but it’s reached it’s retention period and you destroy it, you can’t lose it, it can’t be breached, there can’t be unauthorized access or inappropriate disclosure.

Privacy Program and Records Retention Intersect

- Breach Notification – example:
  - < 150 individuals = 60+ Hours
- GDPR – requirement to only keep personal data for as long as needed for the purpose for which it was collected (and in compliance with federal/state law).
  - If you collect personal data on EU data subject employees and it has reached the end of the retention period and you don’t destroy it, and it gets compromised, GDPR can impose HUGE fines and penalties.

Special Consideration for Electronic Records

- Electronic records are considered records and retention requirements apply equally to them.
- Much more difficult to manage – but proper management is critically important.
- Special Considerations include (not limited to):
    - Access electronic records for the duration of their life – sometimes those records are maintained using obsolete technology – if they have a permanent retention requirement, they may need to be converted as technology changes.
    - Access controls and integrity monitors must be implemented to prevent alterations, unauthorized access, use and disclosure.
    - Information security controls – physical, administrative and technical – to prevent misuse or breaches.
    - Ability to destroy records when they reach the end of the retention period. Easy to just let them sit there but they need to be destroyed just like paper.

Special Consideration for Electronic Records

- This applies to electronic records regardless of where they are stored.
  - Shared Drives
  - Software Applications (PeopleSoft, Banner, etc.)
  - File Management Systems (Webxtender)
  - File Sharing Locations (OneDrive, Sharepoint)
    - Restrictions… PRIVACY MATTERS

Special Consideration for Electronic Records

- Scanning is ok BUT….
  - Paper records can be scanned, saved electronically and the paper can be destroyed only:
    - The paper record is not required to be retained in its original form
    - The paper record contains ”wet signatures” and those signatures are required under a regulation or university policy
    - There isn’t a regulation that prohibits it
    - There is a quality control system in place to ensure that the scanned document is legible
    - The scanned version is retrievable and reproduceable if needed

Special Consideration for Email

- Email is a record – retention requirements apply.
- They can be kept in email format as long as all the other retention, privacy and security requirement are met.
- Email that is not required to be kept should be deleted when no longer needed for administrative purposes.
- DO NOT transmit protected or regulated data using email. Use secure file transfer.
    - https://filetransfer.uvm.edu/send/
- If you don’t need to download attachments that contain protected or regulated data, don’t.
- If you need to download these, make sure they are (1) safeguarded and (2) saved in such a manner that they can be deleted when they reach the end of their retention period.

Special Consideration for Archival Records

- Records documenting UVM's history strategic decisions, organizational changes as well as some official publications may be archival records.
- If you feel a unique record may hold archival value, contact the University Archivist prior to disposing.
    - https://specialcollections.uvm.edu/collections/archives

Special Consideration for Litigation Holds

- WHEN NOT TO DESTROY…
    1. Pending anticipated litigation
    2. External investigation
    3. Internal audit or investigation
    4. Attorney/Client Privileged Compliance Investigation/Review
    5. Pending request to see a record
- OGC will send notification for litigation holds but units are required to ensure that records are not destroyed until the hold has been lifted.
- Check with OGC if any of the above occur but you have not received a litigation hold request.

Special Consideration for Public Records Requests

- All requests follow the Records and Documents Request Policy
- Time considerations apply under the Vermont Public Records Act so prompt response is needed.
- Requests must be made in writing.
- All requests go through VP of Executive Operations.

Conclusion

- Remember the four buckets

Conclusion

- Apply retention requirements to all records regardless

  of format

  - Paper, Electronic, Recorded
- Only collect personal and regulated data if necessary and authorized. If collected, SAFEGUARD it.

Conclusion

- Know when to destroy and when not to destroy.
- Know how to respond to a request for information.

Office of Audit, Compliance & Privacy Services

Office of Privacy Services

802-656-3086

privacy@uvm.edu

*Help*Line: (800)-461-9330

University of Vermont