RECORDS MANAGEMENT POLICY

Purpose and Scope of Policy

The Records Management Policy is designed to provide guidance about University records from the time of their creation or receipt to their ultimate disposition. The Records Management Policy applies to all records regardless of media type (*e.g.*, paper, computer data, microfilm, electronic mail, photographs, voice mail, etc.) created at all levels of the University.

The goal of the University is to attempt to make, preserve, and safeguard records that should be retained for legal, operational, or historical reasons, and to encourage disposal of records that are of no further value. Specifically, the University should attempt to:

- Create only the records it needs.
- At a minimum, retain records according to the Records Retention Schedule.
- Maintain records in appropriate storage equipment and locations.
- Limit access to confidential records on a 'need to know' basis.
- Identify and protect vital records.
- Preserve records of historical significance.
- Dispose of records no longer required in the proper manner.

University Records vs. Private Records

The Records Management Policy applies to all University Records. University Records are records that are created or received by officers or employees of Pepperdine University acting in the course and scope of their duties. Such records include not only letters, memoranda, and contracts, but can also include records in an employee's "personal filing system" such as calendar books, expense records, and handwritten notes. Only those records obviously outside the scope of employment (*e.g.*, schedule for club softball team, personal e-mail and junk e-mail) are considered private records.

Responsibility for University Records

The primary responsibility for managing the University's records rests with each department. Each department is strongly encouraged to appoint a records manager to assist with the implementation and compliance with this policy. In addition, each department is strongly encouraged to designate one day or a portion thereof each year to allow its employees to focus on the requirements in the Records Management Policy.

General Records Retention Schedule

A Records Retention Schedule is available at www._____ for your reference. The retention periods in the timetable apply to the official record copy of certain records. Extra copies should be retained until obsolete, superseded, or administrative value lost.

The Schedule is a non-exhaustive timetable stating a recommended retention period. Where possible, it provides the legal authority for a minimum retention period. However, various federal and state laws may not be the only factor to consider when determining the period of time to maintain records. Other policies or certain contracts that Pepperdine has entered into may dictate a retention period. Further, University records may need to be maintained for operational use (*i.e.*, records that are needed so the user can do his or her job). Finally, some records should be maintained for historical reasons.

In addition to these considerations, other factors to take into account when making retention decisions include, but are not limited to: (1) the purpose and importance of the records; (2) how often the records are referred to and/or used; (3) the space availability to store the records; (4) the business necessity of the records; and (5) the needs of each individual office maintaining the records. There are no set answers to these questions. Effective analysis requires a common-sense approach that balances all relevant factors. However, in no event should the records be kept for less time than the period specified in the Records Retention Schedule.

Electronic Records

Electronic records are records that are created, received, maintained, or stored on University local workstations, laptops, hand-held devices such as personal digital assistants (PDA's), or central servers. Examples include, but are not limited to electronic mail, word processing documents and spreadsheets, and databases. Electronic records are subject to the same controls and legal requirements as paper documents. Therefore, maintenance and disposal of electronic records, as determined by the content, is the responsibility of each department and its employees, and should be performed in accordance with this Policy and the applicable University Information Security Policies (currently under review).

Because electronic records are stored in a form that is easy to modify and update, and because it is hard to guarantee that electronic records can continue to be read in the face of changing formats and technologies, electronic records must be administered carefully to assure their accuracy and longevity. Sound business practice suggests: (1) properly naming, filing, and labeling electronic documents; and (2) transferring (when appropriate) electronic records to a more lasting medium/format (especially if long-term accessibility is at issue).

Electronic Mail

Work-related email is a University record and must be treated as such. The content, transactional information, and any attachments associated with the message are considered a record. Management of email is important. Each email user must take responsibility for retaining or disposing of these University records in accordance with this policy. Retention or disposal should be based on the content or purpose served. If email is retained it should be maintained in a format that preserves contextual information and facilitates retrieval and access. Email retained electronically should be stored in a logical filing system. This will assist in deletion of messages once their retention periods expire. Personal email or junk email should be deleted immediately from the system.

Confidential Records

There are certain records that contain highly sensitive information. Confidential records include, but are not necessarily limited to, records containing medically-related information (*e.g.*, physical examination reports, employee-related medical leave documents), trade secrets, attorney-client communications, psychological and/or psychiatric records, social security numbers, financial information including University data and personal financial data, driver's license numbers, or records establishing disability. Confidential records should be stored in a location such that they are accessible only to those who have a genuine 'need to know.' For example, confidential records should be kept in separate, locked cabinets, or in the case of electronic documents, in accordance with the applicable University Information Security Policies (currently under review). Generally, individuals have a genuine 'need to know' where without access he or she would be hindered in the effective performance of University duties. When confidential records have reached the end of their retention period, they should be properly disposed of as soon as practicable.

Extra Copies

Offices retaining convenience copies and/or photocopies of records may recycle those copies when no longer needed for reference. The University encourages the use of the recycling bins located in campus buildings. Copies containing confidential and highly sensitive information should be disposed of in accordance with this policy.

Storing Records

Currently, the University does not have an on-site storage center. You may consider using a third-party storage facility to store records for you. The third-party facility should be able to meet your operational needs and legal requirements. All members of the University contracting with third parties must convey any relevant University information management policies to third party storage contractors, and make privacy and security obligations of those contractors enforceable by contract. When storing records in boxes -- whether paper or electronic -- you should consider *adequate space and accessibility* (when records are stored, you must still maintain control over them), *security* (allow only approved people to access the storage facility pursuant to proper logging of activity), *temperature and humidity control* (proper temperature and humidity control are essential for preserving electronic records on digital media as well as paper records), and *damage prevention* (pest infestation, smoke, sprinkler damage, etc.). Records that are stored in boxes should be clearly marked with a description or workable code that is sufficiently effective to retrieve the information later, if necessary (*not* "various office records"). Stored records should be properly disposed of as soon as possible when they become due for disposition.

Scanning

Scanning offers an alternative storage medium to paper records that must be maintained for a long period of time and/or permanently. Scanning capability varies University wide. Departments have the option of scanning documents through departmentally owned or accessible scanning hardware or through contracting with an outside scanning service. All outside scanning service providers used for records containing confidential information should be aware of any relevant University Information Security Policies (currently under review), and privacy and security obligations of the contractors should be enforceable by contract. Records that are scanned should be properly disposed of when they become due for disposition.

Archiving Records

The University's archivist can be reached at extension 4434. Due to limited space, not all documents that must be archived can be stored in Payson Library. The University archivist is available to review records to determine their archival value and/or to provide advice regarding the necessary supplies to properly archive materials.

Disposal of Records

Normally, records should be properly disposed of when the period specified in the Records Retention Schedule ends. When large quantities of records are disposed of; for example, in connection with an annual review of departmental files, each department should complete and permanently retain a Destruction of Records Form, available at www._____.

Generally, confidential records and records containing personally identifiable information (e.g., social security number, payroll information, IRS information, benefits, etc.) should be disposed of by shredding so that they cannot be read or reconstructed. Confidential

electronic records should be "wiped" clean ("deleting" of computer files or other electronic records is not acceptable) or the storage media, e.g., floppy discs, CD-Roms, and computer hard drives, physically destroyed. An electronic record is "wiped" clean when it is rendered permanently unavailable. Methods to "wipe" clean electronic records include electromagnetic erasure, use of software to overwrite the record with a single character, or data scrambling. Each department should consult with Information Technology or the University Computer Clean-up and Disposal Policy (currently under review) to determine the most appropriate methods of destruction.

Information Technology Backup Files

Information Technology performs backups on a regular schedule of the e-mail and electronic files stored on central servers for disaster recovery. The purpose of the backups is to provide a means to restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster. Therefore, even though electronic records may still reside on the University's backup media after deletion and until recycled or destroyed in the normal course of business, backup media is to be used for system restoration purposes only.

Potential or Pending Litigation, Government Investigation or Audit

Records due for disposal should be put on "hold" at the slightest hint of, or during any pending, litigation (including instances where the University may be a plaintiff), government investigation, or audit. Such records should not be disposed of until the issue is resolved.

Destruction, Alteration, or Falsification of Records

The law holds all of us responsible for the deliberate destruction of documents when litigation, government investigation, or audit is foreseeable. For example, it is a crime to knowingly alter, destroy, mutilate, conceal, cover up, falsify or make a false entry in any record, document or tangible object with the intent to impede, obstruct, or influence an investigation. Further, it is a crime to corrupt, alter, destroy, mutilate, or conceal a record, document or other object or attempt to do so with the intent to impair the object, integrity, or availability for use in an official proceeding.

Violations

Violations of the law or of the Records Management Policy may result in disciplinary action, up to and including dismissal. Further, if records are deliberately destroyed in violation of the law, significant criminal or civil penalties may be imposed.

Last modified September 15, 2006.