Policy Statement
Golden Gate University requires that its records be managed in a systematic and logical manner according to plans developed by the departments that maintain those records, and consistent with applicable law.

Reason for Policy/Purpose
The University is committed to effective records management including meeting legal standards for record retention and protection of privacy, optimizing the use of space, minimizing the cost of record retention, and properly destroying outdated records. This policy applies to all records, regardless of whether they are maintained in hard (paper) copy, electronically, or in some other fashion.

Who Needs to Know This Policy
Faculty and staff

Policy/Procedures
Federal, State and City regulations require that the University adhere to numerous record retention mandates. The appropriate time periods for record retention are fact specific and subject to ongoing statutory and regulatory changes. Therefore, each department must develop its own records management plan in cooperation with the Office of the Vice President of Business Affairs.

Retention and Maintenance of Records
The University requires that its records be maintained in a consistent and logical manner and be managed so that the University:
1. Meets legal standards for protection, storage and retrieval;
2. Protects the privacy of faculty, staff, and students of the University;
3. Optimizes the use of space;
4. Minimizes the cost of record retention; and
5. Destroys outdated records in an appropriate manner.

Departments that maintain University records are responsible for establishing appropriate records management procedures and practices. Each department’s administrative director, manager, or designee must:
1. Be familiar with the University’s Records Management Policy;
2. Develop the department’s and/or office's record management procedures and practices, consistent with this policy;
3. Educate staff within the department in understanding sound record management practices;
4. Restrict access to confidential records and information; and
5. Coordinate the destruction of records as provided in the applicable procedures.

The Office of the Vice President of Business Affairs is available to work with individual departments to implement these requirements. Faculty and staff should feel free to address questions about retention and destruction schedules to this office.

Confidentiality Requirement
Many records subject to record retention requirements contain non-public confidential data. Such records are protected by federal, state and local statutes, including the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley (GLB) Act, and the Health Insurance Portability and Accountability Act (HIPAA). In addition to the statutory requirements, any record that contains confidential data should be treated in accordance with the University’s privacy and security policies (see the Related Information section of this policy).

Electronically Stored Information
Recent years have witnessed a tremendous growth in the use of electronically stored information (“ESI”) by the University. The ease with which ESI may be created, the number of places where ESI may be stored, and new rules regarding the use of ESI in litigation, all require that the University manage its ESI effectively, efficiently and consistent with its legal obligations. Accordingly, departments must include ESI in the development of their records management plans.

Preservation of Records Relevant to Legal Matters
Any record that is relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation or enforcement action shall be retained at least until final resolution of the matter. In these circumstances, the Offices of the Vice President of Business Affairs will notify relevant departments and work with staff to identify and preserve any records (including electronic records) and other information that could be relevant to the matter. This situation will include a directive that the relevant unit’s normal document destruction policies or protocols temporarily be suspended. Employees who become aware that an investigation or legal proceeding has commenced or is anticipated against their department or unit promptly must notify the Office of the Vice President of Business Affairs, so that all records with potential relevance to the investigation or legal proceeding can be preserved as necessary.

It is an obstruction of justice offense to destroy, falsify, or alter any records or documents in order to impede a federal investigation. If any employee is asked to falsify, destroy, or alter any records, he or she should immediately inform senior management or the board of directors, if a member of senior management is involved in the offense.

Disposal and Destruction of Records
Disposal and destruction of records must follow the University’s Records Management Policy, and with the records management practices and procedures applicable to the department. Records can be destroyed in one of the following ways:
1. Recycle non-confidential paper records;
2. Shred or otherwise render unreadable confidential paper records (BSF can assist in effectively disposing of this data); or
3. Erase or destroy electronically stored data. (ETS can assist in effectively disposing of this data.)

Questions about responsibilities should be directed to the administrative manager or department designee. For additional assistance please contact the Office of the Vice President of Business Affairs.

Definitions

Confidential Data
Confidential Data is information protected by statutes, regulations, University policies or contractual language. Managers may also designate data as Confidential. By way of illustration only, some examples of Confidential Data include:

- Medical records
- Student records and other non-public student data
- Social Security Numbers
- Personnel and/or payroll records
- Bank account numbers and other personal financial information
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Confidential Records
Records that contain confidential student or employee data that should have limited access and be protected from inadvertent disclosure.

Record
Information that has been recorded in some fashion and can be retrieved. It can be an original document, photograph, blueprint, sound or video recording, microfilm, or electronically maintained.

Responsible Department
The department designated as having the responsibility for retention and timely destruction of the particular types of University records in their control.

University Record
The original or a copy of any record. These can be either electronic or paper and were either received or created by the department.

Related Information

Legal References
Gramm-Leach-Bliley Financial Modernization Act, P.L. 106-102
Health Insurance Portability and Accountability Act, P.L. 104-191

 Approving Authority
To be approved by the Audit Committee on May 7, 2009