

## RECORDS MANAGEMENT POLICY

### I. Policy Section

3.0 College Operations

### II. Policy Subsection

3.6 Records Management Policy

### III. Policy Statement

Grand Rapids Community College 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 state and federal laws.

### IV. Reason for the Policy

Grand Rapids Community College is committed to effective records management including meeting legal requirements for record retention and privacy protection, optimizing the use of space, minimizing the cost of record retention, and properly destroying outdated records. This policy applies to all records, including but not limited to documents maintained in hard (paper) copy, electronically, or in some other fashion.

### V. Entities Affected by this Policy

Board of Trustees  
All GRCC Employees

### VI. Who Should Read this Policy

All GRCC Employees

### VII. Related Documents

Family Education Rights to Privacy Act (FERPA)  
Health Insurance Portability and Accountability Act (HIPAA)  
Gramm-Leach-Bliley Act (GLBA)  
GRCC's Personally Identifiable Information Policy  
State approved Records Retention and Destruction Schedule

### VIII. Contacts

Policy Owner: General Counsel

IX. Definitions

1. Confidential Data: information protected by statutes, regulations, College policies or contractual language. Managers may also designate data as confidential. Confidential Data includes but is not limited to:
  - a. Medical records
  - b. Student records and other non-public student data
  - c. Social Security Numbers
  - d. Personnel and/or payroll records
  - e. Bank account numbers and other personal financial information
  - f. Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.
  - g. Information defined as protected Personally Identifiable Information as set forth in the College policy.
2. Confidential Records: Records that contain confidential student or employee data that should have limited access and be protected from disclosure except as required by law.
3. Record: Information that has been preserved in a storage medium and can be retrieved. A record includes but is not limited to paper, electronic or microfilm documents, photographs, blueprints, or audio or video recordings created or received by employees in connection with transactions of College business and which are retained by employees as evidence of the activities or functions of College business.
4. Responsible Department: The department designated as having the responsibility for retention and timely destruction of College records in their control.

X. Procedures

The College is subject to Federal and State laws regarding record retention and disposal. Each department is required to develop a records management plan consistent with this policy and all applicable State and Federal laws and regulations and must submit this plan for the particular records it maintains to the Office of the General Counsel for approval by the state.

1. Retention and Maintenance of Records

The College requires that its records be maintained in a consistent and logical manner and be managed so that the College:

- a. Meets legal standards for protection, storage, retrieval and disposal;
- b. Protects the privacy of faculty, staff and students as required by law;
- c. Optimizes the use of space;
- d. Minimizes the cost of record retention; and
- e. Destroys outdated records in an appropriate manner.

Departments that maintain the College's records are responsible for establishing appropriate records management procedures and practices. Each department's administrative manager or a designee must:

- a. Be familiar with this policy;
- b. Develop the department's and/or office's record management procedures and practices, consistent with this policy;
- c. Educate staff within the department in understanding sound record management practices;
- d. Restrict access to confidential records and information; and
- e. Coordinate the destruction of records as provided in the applicable departmental procedures.

The Office of the General Counsel is available to work with individual departments to implement these requirements.

## 2. 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 statutory requirements, any record that contains confidential data should be treated in accordance with the College's privacy and security policies (see the Personally Identifiable Information Policy).

## 3. Electronically Stored Information

Electronically stored information ("ESI") must be managed by the College effectively, efficiently and consistent with legal obligations. Accordingly, all departments must include ESI in the development of their records management plans.

## 4. 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 Office of the General Counsel will notify relevant departments and work with employees to identify and preserve any records (including electronic records) and other information that could be relevant to the matter. This will include a directive that the relevant department's normal document destruction policies or protocols temporarily be suspended as the stop destruction notice requires. Employees who become aware that an investigation or legal proceeding has commenced or is anticipated involving their department must promptly notify

the Office of the General Counsel, so that all records with potential relevance to the investigation or legal proceeding can be preserved as necessary.

5. Disposal and Destruction of Records

When the College receives approval by the State of a comprehensive Records Retention and Destruction Schedule it is appropriate to dispose of records, they can be destroyed in one of the following ways:

- a. Recycle non-confidential paper records;
- b. Shred or otherwise render unreadable confidential paper records; or
- c. Erase or destroy electronically stored data. (Information Technology can assist you in effectively disposing of this data.)

XI. Forms

N/A.

XII. Effective Date

March 18, 2013

XIII. Policy History

This is a new policy created to address record management.

XIV. Next Review/Revision Date

March, 2017