GOUCHER | college

Written Information Security Program
Frequently Asked Questions

1. What is the purpose of the policy?

The purposes of the policy are to:

- Establish a program to protect the confidential data of students, alumnae, faculty and other employees of the College;
- Establish employee responsibilities for safeguarding confidential data; and
- Outline procedures to implement and administer this program, including administrative, technical and physical safeguards.

2. Why has Goucher implemented this program?

Data breaches and loss of confidential data have become more commonplace in recent years in many industries, including in higher education.

We have a responsibility to keep the records of our students and employees confidential, and that requires all of us taking responsibility for the protection of confidential data to which we have access.

3. What records should I be concerned about?

You already know that FERPA, the Family Educational Rights and Privacy Act, protects the privacy of student "educational records." These include, with some exceptions for things like directory information, any record maintained by the College or someone acting for the College which is directly related to a student.

The new policy addresses a more limited and sensitive category of documents – what the policy calls **Personal Information** and **Nonpublic Financial Information**. These documents are those documents that link a student's name to some type of sensitive financial information, like a social security number, credit card or bank account number. They also include financial information about a constituent of the College (student, employee, parent, alumni, donor, etc.), such as information that a student provides on an application to obtain a student loan, tax returns, documents that contain billing account balance information, payment history, and credit or debit card purchase information.

NOTE: For purposes of this policy, Personal Information does not include Goucher assigned student identification numbers, although such information should be treated as other student information and is protected under the Family Educational Rights and Privacy Act (FERPA).

4. What are my new responsibilities under this policy?

- To maintain the privacy and integrity of Confidential Data, which includes Personal Information and Nonpublic Financial Information;

- To report to the General Counsel any possible or actual unauthorized disclosure or other compromise of Confidential Data;
- To identify within your work area potential risks to the security and confidentiality of Confidential Data;
- To implement and review safeguards in your work area.

5. How do I do all of that?

Think of these four things:

a. Access

- If you have access to confidential documents in your work area, make sure that only authorized people have access to them; e.g., lock paper records in a file cabinet, lock your office when you leave, even for a few minutes.
- If you are a supervisor, periodically check how your staff is maintaining confidential information. If an employee leaves the college, make sure confidential documents they leave behind are secured.

b. Storage

- Do not use cloud-based storage solutions that are not supported by the College (including DropBox, Microsoft OneDrive, Apple iCloud, etc.). Only use Box or store documents on the departmental drive of the Magellan server.
- ***Do not store Confidential Data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives).***
    - If you choose to store such data on a laptop, that device must be password protected and encrypted, particularly if that device is taken off campus.
- Paper records containing Confidential Data must be kept in locked files or other areas when not in use, and should not be removed from the premises of the College.

c. Removing records from campus

- When it is necessary to remove records containing Confidential Data from campus, do it carefully. Under no circumstances are documents, electronic devices, or digital media containing Confidential Data to be left unattended in any insecure location.

d. Disposition

- Destruction of paper and electronic records containing Confidential Data must be carried out in a way that maintains their confidentiality; i.e., shredding, using a cross-cut or strip shredder, should be used for all documents that contain Confidential Data; alternatively the college contracts with a provider to collect and confidentially destroy confidential paper records.

6. What about electronic records on computers? How can I keep them safe?

- Use unique and strong passwords and change them often. Do not share passwords.
- Do not use email to send Confidential Data such as social security numbers or credit card information.
- Promptly complete online training offered to you that will give you information about how to better protect sensitive information.

7. What about encryption?

Encryption software will be placed on laptop and desktop computers that contain Confidential Data. If you have one of these computers, the office of Information Technology will arrange to place this software on your computer. This applies to most individuals in the following offices:

- Admissions
- Bursar / Billing
- Business Services
- Controller's Office and Accounts Payable
- Counseling Center
- Financial Aid
- Health Center
- Human Resources/Payroll
- Information Technology
- Institutional Effectiveness
- Office for Strategic Initiatives
- Office of Accessibility Services
- Office of Advancement
- President's office
- Registrar's Office

……

Questions about the program can be addressed to the Vice President for Information Technology.