GOUCHER | college

# System Administrator Policy

## I. PURPOSE

The purpose of this policy is to establish the college's expectations for Goucher College employees who have administrative and access rights to the electronic communications, files, or documents of members of the college community.

## II. DEFINITIONS

**Electronic Communications Systems**: Includes, but is not limited to, the use of college computer networks, the Internet, email, telephones, voice mail, video, multimedia, and all other computer-related communications provided by the college. Facilities, technologies, and information resources used for college information processing, transfer, storage, and communications are also included.

**Confidential electronic communications**: Include e-mail, and electronic data, files, or records,

## III. RESPONSIBILITIES OF SYSTEM ADMINISTRATORS

The creation and operation of electronic communications systems require personnel to configure, manage, administer, and monitor computer and other electronic communications hardware and software. System administrators who configure these systems and services and monitor the performance of these systems are responsible for:

A. Setting up accounts for individuals to access information and services.

B. Helping resolve problems with usernames and passwords.

C. Researching and resolving problems.

D. Configuring systems and services to the needs of the organization.

E. Monitoring the performance of systems and services.

F. Taking corrective action to improve performance.

G. Implementing corrections and upgrades to provide new features and enhancements.

H. Identifying internal and external risks to the security, confidentiality, and integrity of information.

I. Evaluating the effectiveness of the current safeguards for controlling security risks.

J. Designing and implementing a safeguards program.

K. Regularly monitoring and testing the safeguards program.

## IV. ACCESS TO ELECTRONIC COMMUNICATIONS AND FILES

All hardware and software associated with the electronic communications systems are the property of the College. The College supports a climate of trust and respect and does not ordinarily read, monitor, or screen email or other electronic data, files, or records. However, the College retains the right, in circumstances described below, to access electronic communications, data, files or records for college-related purposes and members of the college community should therefore have no expectation of privacy with respect to the use of electronic resources.

### A. Immediate health or safety risk

Employees and agents of the College may read, listen to, or otherwise access confidential electronic communications, in order to perform the responsibilities of the job as long as permission to access the confidential contents has been requested by the Office of Campus Safety or the Office of Risk Management due to an immediate risk to the health or safety of people or property.

### B. System maintenance

System administrators of the College may read, listen to or otherwise access confidential electronic communications, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of the job and access is necessary to maintain system integrity, including but not limited to tracking malware, investigating security incidents, and performing ordinary system repair, maintenance and enhancement.

### C. Purposes approved by Office of Risk Management

Employees and agents of the College may read, listen to or otherwise access confidential electronic communications, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of the job and permission to access the confidential contents has been obtained from the College's Office of Risk Management for purposes including but not limited to:

1. Comply with legal requests and demands, search warrants, subpoenas, discovery requests, legislative audits, and other requests for information to which the College is required to respond under law.
2. Perform internal investigations required by federal, state or local law, or college policies or procedures.
3. Obtain information related to the following matters:
    - Actions brought against the College or any of its faculty, staff, or students.
    - Actions brought on behalf of the College or any of its faculty, staff, or students.
    - Situations involving the health or safety of people or property.

### D. Separation from the College

Supervisors must complete a technology separation form. Each supervisor is responsible for ensuring that access to college systems is terminated on the last day of employment and that needed computer files are retained when such a circumstance occurs.

## V. OBLIGATION TO MAINTAIN THE CONFIDENTIALITY OF ACCESSED COMMUNICATIONS

If, in the course of performing responsibilities set forth in section III, a systems administrator encounters evidence that an individual is not using electronic resources in a lawful and ethical manner as outlined in the Computer Use Policy, and/or is breaching the confidentiality of electronic communications in violation of this policy, the administrator must contact the appropriate office: The Office of Student Affairs for suspected student violations; and the Vice President for Human Resources and the Office of Rick Management for employee violations.

## VI. ENFORCEMENT

System Administrators who improperly read, disseminate, or otherwise compromise the confidentiality of electronic mail or other data, files or records are subject to disciplinary action, up to and including dismissal.

## VII. RESPONSIBLE OFFICE

For more information or if you have questions about this policy, please contact the Associate Vice President for Information Technology.

## VIII. HISTORY

Approved by the President on July 15, 2003
Revised: September 24, 2003; December 1, 2003; February 6, 2019; February 16, 2023