Goucher College System Administrator Policy

A. Purpose

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

B. Definitions

For the purposes of this policy, the term "Electronic Communications Systems" includes, but is not limited to, the use of College computer networks, the Internet, electronic mail (e-mail), telephones (including cellular telephones), voice mail, pagers, modems, fax transmissions, 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.

C. 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:

1. Setting up accounts for individuals to access information and services
2. Helping resolve problems with usernames and passwords
3. Researching and resolving problems
4. Configuring systems and services to the needs of the organization
5. Monitoring the performance of systems and services
6. Taking corrective action to improve performance
7. Implementing corrections and upgrades to provide new features and enhancements
8. Identifying internal and external risks to the security, confidentiality, and integrity of information
9. Evaluating the effectiveness of the current safeguards for controlling security risks
10. Designing and implementing a safeguards program
11. Regularly monitoring and testing the safeguards program

D. 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 electronic mail 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.

1. **Immediate health or safety risk**

   Employees and agents of the College may read, listen to or otherwise access confidential electronic communications, including e-mail, and electronic data, files or records, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of his or her job and permission to access the confidential contents has been requested by the Office of Public Safety or Legal Counsel due to an immediate risk to the health or safety of people or property.

2. **System maintenance**

   System administrators of the College may read, listen to or otherwise access confidential electronic communications, including e-mail, and electronic data, files or records, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of his or her job and access is necessary to maintain system integrity, including but not limited to, tracking viruses and performing ordinary system repair, maintenance and enhancement.

3. **Purposes approved by Legal Counsel**

   Employees and agents of the College may read, listen to or otherwise access confidential electronic communications, including e-mail, and electronic data, files or records, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of his or her job and permission to access the confidential contents has been obtained from the college's Legal Counsel, for purposes including but not limited to:

   a. To be compliant 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
   b. To perform internal investigations required by federal, state or local law, or college policies or procedures
   c. To 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

4. **Separation from the college**

   Employees and agents of the College may read, listen to or otherwise access confidential electronic communications, including e-mail, and electronic data, files or records, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of his or her job and such access is required in order to delete or retain any or all electronic mail messages, computer files, or electronic data on the college's systems after a student leaves the College or an employee separates employment. Each supervisor is responsible for ensuring that access to college systems

is terminated and that needed computer files are retained when such a circumstance occurs.

E. Obligation to Maintain the Confidentiality of Accessed Communications

1. A systems administrator shall not read, listen to or otherwise view the confidential contents of any electronic communication unless the administrator needs to access the confidential contents in order to perform the responsibilities set forth in paragraph D hereof.

2. If, in the course of performing responsibilities set forth in paragraphs C and D hereof, a systems administrator encounters evidence that an individual is not using electronic resources in a lawful and ethical manner as outlined in the Goucher College Computer Use Policy, and/or is breaching the confidentiality of electronic communications in violation of this policy, such administrator shall contact the Director of Judicial Programs for suspected student violations and the supervisor for suspected employee violations.

F. 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, including dismissal.

G. Responsibilities and Contacts

Suspected violations and questions about this policy should be reported to the Chief Technology Officer.

H. Policy Effective Date

- Approved by the President on July 15, 2003
- Revised: September 24, 2003
- Revised: December 1, 2003