GOUCHER | college

Electronic Communications Policy

I. PURPOSE

The purpose of this policy is to:

A. Establish electronic mail (email) as an official means of communication within the campus community.

B. Establish guidelines relating to the permissible use of the College's electronic communications systems.

C. Describe the privacy rights of members of the campus community.

D. Define the College's right of access to electronic communications.

E. Describe the intellectual property rights of individuals using electronic communication systems.

F. Establish the College's policy for the retention of electronic communications.

G. Describe the enforcement of electronic communications policy.

II. STATEMENT

Email is considered an official means of communication for Goucher College. Implementation of this policy ensures that students and employees have access to this critical form of communication.

III. DEFINITIONS

Electronic communications systems: Includes, but is not limited to, the use of college computer networks, the Internet, email, telephones (including cellular telephones), voice mail, 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.

IV. EMAIL AS AN OFFICIAL MEANS OF COLLEGE COMMUNICATION

A. College use of email

Email is an official means of communication for Goucher College. Therefore, the College has the right to send communications to students, faculty, and staff via email and the right to expect that those communications will be received and read in two (2) business days of having received the message.

B. Assignment of email addresses

Information Technology will assign an official college email address to all students, faculty, and staff according to the Digital Identity Policy. It is to this official address that the College will send email communications. This official email address will be listed in the address book of the College's email system.

C. Redirecting of email

Users can redirect their email to another email address (e.g., @gmail.com, @yahoo.com) but the College will not be responsible for the handling of email by outside vendors.

D. Expectations regarding use of email

In recognition that certain communications may be time-critical, students, faculty, and staff are expected to respond to all emails directed personally to them within two (2) business days of having received the message. If an employee´s work schedule does not permit them to answer the email inquiry within two days, the employee should indicate when they will be able to respond.

E. Educational uses of electronic communication

Faculty should discuss with their students how assignments and documents are to be submitted. Faculty may expect that students' official email addresses are being accessed, and faculty may use email for their courses accordingly.

F. Using email securely

Users should practice caution before opening attachments or clicking links in email messages from external sources that contain certain indicators of suspicion including urgent calls to action for account credentials or funds, or regarding imminent loss of access or loss of funds or other harm.

V. PERMISSIBLE USES OF ELECTRONIC COMMUNICATIONS

The College provides electronic communications services for students, faculty, and staff for use when engaging in activities related to teaching, learning, and the operations of the College. Faculty and staff should be using their Goucher email for Goucher business. Faculty and staff should use a personal email address for personal business and correspondence.

The College has no control of the addressing of incoming email. If an employee receives an email that should have been transmitted to another employee, the email message should be forwarded to the proper party or returned to the original sender with an explanation. No employee should respond to an email request belonging to another party unless the employee has been authorized to do so.

The College will take reasonable precautions to ensure the security and appropriate use of electronic communications systems; however, the College accepts no responsibility for harm caused directly or indirectly using the College's electronic communication systems as a result of the user's negligence.

College email shall not be used for illegal or wrongful purposes, including but not limited to the following:

1. To communicate, to access, or to disclose information in violation of any copyright, patent, license agreement, or other intellectual property right.
2. To communicate, to access, or to disclose information in violation of applicable laws and regulations.
3. To communicate obscene, defamatory, harassing, or threatening information.
4. To communicate anonymously or under a pseudonym or to conceal or misrepresent a user's identity.
5. To compromise the integrity, security, or efficient and proper operation of college email, including but not limited to obtaining or attempting to obtain unauthorized access to other users' files, or to other networks or systems.
6. To intentionally run or install on any system or network a program or other electronic device that the user knows may damage a computer system or network, including but not limited to programs known as computer viruses, Trojan horses, worms, or other malware.
7. To use email to transfer executable files or other software and install them on lab computers.
8. To send unsolicited emails to large numbers of people to promote products or services.

The College's email system scans all email being sent to determine if the email contains sensitive information. If the email system detects a social security number or a credit card number, the email will be prevented from being sent and a message will be provided that sensitive information was detected. Sensitive information should not be sent through email.

In addition, users are expected to accept and comply with the individual responsibilities relating to computer and information technology as set forth in the Goucher College Computer Use Policy.

VI. PRIVACY RIGHTS

A. Family Educational Rights and Privacy Act (FERPA)

Personal identifiable information about students contained in email communications or attachments thereto, including information contained in student education records, medical information, and information about disabilities, may be protected by FERPA. When communicating such information about a student via email, parties should consult the College's policy on FERPA and ensure that they have obtained the appropriate consent to communicate such information to another individual.

B. Medical records

Maryland State and Federal laws govern the confidentiality of medical records and prohibit the disclosure of such records without the consent of the individual, except in certain circumstances.

Users of email should obtain all consents required by law when communicating medical information via email about any employee, student, or other person, and otherwise maintain the confidentiality of such information, as required by law.

NOTE: In some circumstances, the provisions of federal law, including the U.S. Patriot Act, may override the provisions of FERPA and state confidentiality laws and permit federal officials to have access to ordinarily confidential records.

VII. COLLEGE ACCESS TO ELECTRONIC COMMUNICATIONS

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.

College employees who improperly read, disseminate, or otherwise compromise the confidentiality of email or other data, files, or records, or who improperly authorize such activities are subject to disciplinary action, including dismissal as outlined in the Goucher System Administration Policy.

A. Immediate health or safety risk

Employees and agents of the College may read, listen to, or otherwise access confidential electronic communications, including email, 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 their job and permission to access the confidential contents has been requested by the Office of Risk Management or the Office of Campus Safety, 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, including email, 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 their job and access is necessary to maintain system integrity, including but not limited to tracking viruses and performing ordinary system repair, maintenance, and enhancement.

C. Purposes approved by the Office of Risk Management

Employees and agents of the College may read, listen to, or otherwise access confidential electronic communications, including email, 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 their job and permission to access the confidential contents has been obtained from the College's Director 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 by law.
2. Perform internal investigations required by federal, state, or local law.
3. Perform internal investigations outlined in college policies.
4. Obtain information related to legal actions brought against the College, such as a breach of contract claim or a discrimination claim.
5. Obtain information related to legal actions brought on behalf of the College such as a dispute with an outside contractor.

D. Separation from the College

It is the policy of the College to deactivate faculty and staff email accounts on the last day of employment at the College.

When employees or students leave the College, supervisors and other agents of the College may read, listen to, or otherwise access confidential electronic communications, including email, and electronic data, files, or records, provided that the supervisor or agent needs to access the confidential contents in order to perform the responsibilities of their job and such access is required in order to delete or retain any or all email messages, computer files, or electronic data on the College's systems. 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.

NOTE: Alumni retain their Goucher email account.

VIII. INTELLECTUAL PROPERTY

In the event that there is a dispute regarding intellectual property that is owned by a member of the College community and maintained or communicated in electronic form through college systems, the College shall have the right, upon written notification to the individual, to obtain access to the work for the purpose of resolving the dispute or determining whether the College has an interest in the property. The Vice President of each division, however, must approve of any such access in writing.

IX. RETENTION OF ELECTRONIC COMMUNICATIONS

The College does not maintain centralized or distributed archives of all email or voice mail sent or received.

Email users should be aware that generally it is not possible to assure the longevity of email records for record-keeping purposes, in part because of the difficulty of guaranteeing that email can continue to be read in the face of changing formats and technologies, and in part because of the changing nature of email systems.

Email users and those in possession of college records in the form of email are cautioned, therefore, to be prudent in their reliance on email for purposes of maintaining a lasting record. Email should be transferred to a more permanent medium when required by college or departmental record retention policies.

X. ENFORCEMENT

The use of electronic communications for illegal or unethical purposes, for abusive and harassing activities (or similar violations of the rights of others), or for purposes inconsistent with college policy or regulation, may result in:

A. Administrative Action

Violations may result in the revocation or restriction of electronic communications access.

B. Disciplinary Action

Violations may result in disciplinary action outlined in the Student Code of Conduct and college policies and procedures.

C. Dismissal

Violations may result in dismissal from the College.

D. Legal Action

Alleged violations may also be referred to local, state, and/or federal authorities.

Suspected violations of this policy by students should be reported to the vice president and dean of students. Suspected violations by faculty should be reported to the provost. Suspected violations by staff should be reported to their immediate supervisor and/or the office of human resources.

XI. RESPONSIBLE OFFICE

Questions about this policy should be directed to the Associate Vice President for Information Technology.

XII. HISTORY

Created on November 1, 2004. Updated on August 5, 2008, September 30, 2019, August 2020, and February 2023.