GOUCHER | college

Computer and Data Use Policy

I. PURPOSE

Goucher College provides computing and networking resources to students, faculty, and staff for teaching, learning, and the operations of the College. Information Technology (IT) personnel maintain and update these resources to support the educational goals of the College. These resources are limited, and how each individual uses them may affect the work of other members of the community and beyond, as our campus network is connected (through the Internet) to other networks worldwide. It is important that all members of the campus community be aware of the proper use of these resources.

II. SCOPE

This policy applies to all Goucher College technology resources and to all users of Goucher College technology resources, including faculty, staff, students, IT personnel, guests, and other users authorized by the College. Personal equipment connected in any way to the college network is also subject to this policy. Users must abide by all applicable restrictions imposed by this policy and by law, whether or not those restrictions are configured in the technology resources and whether or not a person could circumvent them by technical means. In addition, student users must abide by the provisions of Goucher's Student Code of Conduct.

III. PROCEDURES

A. Access to Electronic Communications and Files

Users should be aware that their use of college computing and technology resources is not private, however, 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. The College does retain the right to access electronic communications, data, files, or records for college-related purposes under appropriate circumstances: (a) immediate health or safety risk; (b) system maintenance; (3) purposes approved by legal counsel; and (d) separation of a user from the College. Goucher does not permit the inspection of email, activity, or files by system administrators except under appropriate circumstances outlined in the Goucher System Administrator Policy. 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.

B. Security

Goucher College employs measures to protect the security of its computing resources and of its user accounts. Users should be aware that the College cannot guarantee such security.

Users should engage in safe computing practices by:

- Protecting accounts by not sharing passwords with others, writing down passwords, or sending passwords by email. Neither students nor employees may share passwords with anyone else: other students or employees, family members, student workers, professors, instructors, resident assistants, teaching assistants, counselors, or visitors and other individuals not affiliated with the College. If a student provides their password to parents for purposes of giving them access to the student's Learning Management System account, this will violate the rights of other students in the class under the Family Educational Rights and Privacy Act (FERPA), because this gives an external party access to another student's records in which they do not have a legitimate educational interest. Similarly, if another person learns the user's password, that individual has the ability to access e-mail, personal files, and other system accounts, which may contain sensitive and/or confidential information to which they should not have access.
- Using 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.
- Changing their password and contacting the Help Desk if a user suspects that their password may have been compromised.
- Logging out or locking computers when not in use.
- Not installing potential malicious software or software not approved by Information Technology.
- Installing and maintaining antivirus software on personal computers.
- Promptly reporting any misuse or violations of this policy.

C. Protection of College Data

As part of our commitment to ensuring the integrity and security of college data, all members of the Goucher College community are required to adhere to the following guidelines:

1. Storage Locations: Sensitive data, including but not limited to Social Security Numbers, birth dates, credit card numbers, student information protected by the Family Educational Rights and Privacy Act (FERPA), and student information protected by the Health Insurance Portability and Accountability Act (HIPAA), should only be stored on Goucher network storage, such as the MAGELLAN storage server, or Goucher-approved cloud storage solution, Microsoft OneDrive.
2. Prohibited Storage Locations: For security purposes, the storage of sensitive data on Goucher-owned or personal equipment hard-drives is strictly prohibited. Additionally, the use of personal cloud storage systems for storing sensitive data is not allowed.
3. Data Access Control: Access to sensitive data must be restricted to authorized personnel only. Ensure that access controls, such as password protection and user permissions, are in place to prevent unauthorized access.
4. Reporting Security Incidents: In the event of a security incident or data breach, users must promptly report the incident to the IT department. This includes any loss, theft, or unauthorized access to devices or data containing sensitive information.
5. Training and Awareness: All users handling sensitive data are required to undergo regular training on data security best practices. This training will cover topics such as data encryption, secure data disposal, and recognizing and reporting security threats. IT will coordinate and provide this training.

D. Privacy

Goucher systems and services may not be used to invade the privacy of others. The ability to gain access to another person's account does not imply authorization to do so. As noted in Section III.B, to ensure privacy, accounts and passwords may not be shared with, or used by, people other than those to whom they have been assigned by the college. The following may be grounds for sanctions:

- Accessing another user's account without permission or authorization.
- Providing your username and password to another person.

See Enforcement Section below.

E. Appropriate Use

Goucher's computing and information technology resources, facilities, and services are to be used for purposes congruent with the College's educational mission.

F. Inappropriate Use

Unless expressly authorized by the Office of Information Technology, these resources **cannot** be used for:

- Commercial or political activities.
- Charitable solicitations for non-Goucher related activities.
- Personal business of faculty and staff. Faculty and staff should use Goucher computing resources only for the business of the College. Personal correspondence and file storage should be conducted using personal accounts and resources. **It is the policy of the College to deactivate faculty and staff email and file storage accounts on the last day of employment at the College.**
- Sending unsolicited emails to large numbers of people to promote products or services.
- Engaging in peer-to-peer file sharing, crypto-currency mining, and/or other commercial, profit-based endeavors.
- Use of Tor (aka The Onion Router) is expressly prohibited.

G. Lawful and Ethical Manner

Users of Goucher's technology systems must use the system in an ethical and legal manner and in accordance with Goucher's policies and procedures. Failure to do so may result in disciplinary action under Goucher procedures or prosecution under various federal or state statutes. Some examples of unlawful and unethical manner are:

- Usage of the system to harass, discriminate against, defame, or invade the privacy of any member of the college community or individuals outside the community.
- Usage of the system to send or receive obscene or pornographic materials.

H. Within the Finite Capacity of College Computing and Network Resources

Users must respect the finite capacity of college computing and network resources and limit use to a reasonable amount as determined by the Office of Information Technology. If an individual's use is interfering unreasonably with the activity of others, the College may require that person to limit or refrain from specific uses. Some examples are:

- Excessive/abusive utilization of bandwidth negatively impacting network performance for the campus community.
- Late return of laptop to kiosk during specified time listed in agreement.
- Return of college-issued equipment later than the last day of full-time employment.
- Storing personal video, still pictures, or other large files on college-issued computing resources including MAGELLAN, Box, OneDrive, email, etc.

Goucher is not responsible for backing up files or recovering lost data stored on any desktop computer, laptop computer, or other device. It is the responsibility of the user to protect their data using regular backup and file storage procedures. MAGELLAN department drives are backed up by Goucher every night and files stored on college cloud storage are backed up multiple times per day.

I. Wireless Technology

Goucher College will continue to evaluate and implement wireless technology to enhance teaching, learning, and campus life. However, the College reserves the right to restrict the use of wireless devices in college-owned buildings and all outdoor spaces on the campus for security purposes or if devices are interfering with campus technologies. If you are considering utilizing wireless technology and have questions concerning its use, please contact the Information Technology Help Desk at 410-337-6322.

Not Permitted:

- Wireless routers
- Range extenders

Permitted but Not Recommended:

- Wireless printers (must use USB connection and not a wireless connection)
- Wireless home automation devices (e.g., to turn on/off lights)

J. Care of Equipment

The College expects that members of the campus community will take care of equipment provided to faculty, staff, and students including taking measures to secure equipment from theft. Acts which damage computing resources, deny service to other users, or compromise the integrity of the security systems of the resources are prohibited. Some examples include:

- Physical damage to unsecured equipment, whether accidental or not. Repairs or replacements of damaged equipment are the responsibility of the individual employee, department, and/or division. Students are individually responsible for physical damage to equipment.

- Installation of unapproved software without prior consent of the Information Technology Help Desk. Rights to install software will be rescinded if multiple incidents related to unauthorized installations occur.
- Not protecting personal equipment used to connect to Goucher network. Personal equipment that poses a threat to Goucher resources will be denied access to the network.
- Tampering with or vandalizing network configuration settings and/or physical equipment such as network access points will result in disciplinary action.

If the equipment is lost or stolen, immediately notify your local law enforcement agency. If you are on campus, Campus Safety is your local agency.

K. Copyright

1. Abide by copyright laws and policies

Users must abide by all applicable laws and college policies (e.g., Copyright, Intellectual Property) to protect the copyrights and intellectual property rights of others. Copyrighted works may include texts, cartoons, articles, photographs, songs, software, graphics, and other materials. Users should be aware that many materials available through the Web are protected by copyright. It is the responsibility of the user to assume that materials found on the Web are copyrighted unless the materials contain an express disclaimer to the contrary. Users must obtain permission of the creator or publisher to copy or use software or other copyrighted materials written or created by others and must abide by contracts and agreements controlling installation and use of such software and other materials.

2. Observe restrictions on the use of pictures and video

Users may not display audio, video, or other multimedia images or recordings of people on a web page or on other computing resources without the permission of the people involved. An individual's right to privacy includes the right to restrict the use of personal images. Further, the image may be protected by copyright.

L. Enforcement

Violations of this policy may result in disciplinary action, including but not limited to the restriction of access to college resources, termination of employment, or, in the case of a student, probation, suspension, or dismissal from the College and legal action as appropriate. Cases against students follow the procedures outlined in the Student Code of Conduct.

IV. RESPONSIBLE OFFICIAL

The Office of Information Technology is responsible for communicating this policy to the Goucher user community. Any questions about this policy should be directed to the Information Technology Help Desk (helpdesk@goucher.edu).

V. HISTORY

Reviewed: October 2019; July 2021; August 2022; January 2024.