Network Use Policy

Network Use Policy

Policy Owner	Chief Information Officer
Contact Information	Gavin Foster, Chief Information Officer; gfoster@gettysburg.edu
Approval Authority	Approval Authority: President
Approved By	Robert Iuliano
Approval Date	January 6, 2026
Effective Date	January 2026
Date of Last Review	2001, 2021
Date of Next Review	January 2029
Related Policies	- Acceptable Use Policy - Email Usage Policy - Access to Electronic Information Policy - Information Management Policy - Freedom of Expression Policy - Gettysburg College Access to Electronic Information Policy - Employee Code of Conduct - Community Standards

Network Use Policy

Purpose of Policy

The purpose of the Gettysburg College Network is to support the College's mission. Gettysburg College provides a campus computer Network, including access to the Internet, to advance the educational goals and purposes of the College.

Use of the Network by Users is governed by this Network Use Policy and is subject to all applicable federal, state, and local laws, as well as the rules and regulations of the College.

Scope of Policy

This policy applies to all Users of the Network and to all information transmitted by or at rest on devices attached to the Network.

Definitions

Authorized College Staff: Any employee approved by the Chief Information Officer, including Information Technology employees.

Network:

- Gettysburg College Wired Network: Uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network.
- Gettysburg College Wireless Network: Allows devices to stay connected to the Network but roam untethered to any wires.

System: a collection of hardware, software, and data that work together to perform tasks.

User: A Network User is any person who uses the services provided by Gettysburg College's computer Network.

Policy Description

Privileges of Users:

Access: All Users of the Gettysburg College Network will be granted equitable access to Network resources and services, to the extent permitted by available technology and Network capacity.

Intellectual Freedom: Use of the Gettysburg College Network must comply with the College's Freedom of Expression policy. Except for official statements from appropriate College officers, Gettysburg College does not endorse any opinions stated on the Gettysburg College Network.

Protection from Harassment: All Users are encouraged to communicate individual and differing perspectives. Users are also, however, entitled to work and live in an environment free from harassment. Therefore, any Gettysburg College Network activity that violates the College's harassment policies as defined in the Employee Standards of Conduct policy or as defined in the Community Standards is prohibited.

The Gettysburg College Network and other digital resources may not be used to create, store, or transmit malicious, harassing, or defamatory content of any kind. While in public, shared, or other communal areas and facilities, Network Users must also take care not to display on workstations, computers, or other devices – regardless of whether they are owned by the individual Network User, or owned or provided by Gettysburg College – any images, sounds, messages, or other media or content which could create an atmosphere of hostility or harassment for others.

Network Users must also refrain from using the Gettysburg College Network to transmit to others, in any location, any inappropriate, messages, images, sounds, videos or other media that are or are intending to be threatening, hostile, or harassing in contradiction to the Gettysburg College employee or Community Standards.

Use of anonymity in any form of electronic or digital communication for fraudulent purposes or with the intent to harass another, misrepresent oneself as another is prohibited.

III. Responsibilities of Network Users

Permitted Use:

Use of the Gettysburg College Network for any and all purposes must comply with applicable Federal, state, and local laws and College policies.

Account Responsibility:

Access to the Network is through individual accounts with password protection. Accounts and passwords are not to be shared with any person or party for any reason. All Users are required to complete security training when requested to do so. This training provides the information needed to protect passwords and other credentials and to secure Network resources against unauthorized use or access. Users are expected to make reasonable efforts to complete this training in a timely manner. Users who fail to complete required training may face penalties or disciplinary action. Users are expected to configure and protect their electronic devices and other hardware and software in a way that reasonably prevents unauthorized users from accessing the Network and other resources using College credentials. Users are individually responsible for the appropriate use of all digital resources owned by, assigned, or allocated to them; therefore, Users are accountable to Gettysburg College for all use of such resources. All policy violations which can be traced to an individual account will be treated as the sole responsibility of the owner of that account.

Network Degradation:

The running of programs, services, systems, processes or servers by a

single user, or group of users, that may substantially degrade Network performance or accessibility is not allowed. Use of the Network and its resources to transmit electronic chain letters, mail bombs, malware, viruses, spam or phishing is strictly prohibited. Gettysburg College reserves the right to set limits on an individual User's use of resources through quotas, time limits, and other mechanisms. The College may also lock accounts or remove devices from the Network if they pose a risk to the availability of Network resources for those who need them. Gettysburg College will not be liable to any User for limitations set on their use of Network Resources.

Copyrights:

Users must respect all copyrights and intellectual property laws and always provide proper attributions of authorship. Commercial software licensed to Gettysburg College may be installed only on equipment and devices expressly covered by those licenses. Individuals who have software licensed to them and installed on a Gettysburg College computer shall produce original documentation to verify compliance upon request from a network administrator. The installation, activation, and/or use of unlicensed software, or the use of software in a manner that exceeds the scope of the license, is prohibited within the Network and on any devices owned or maintained by Gettysburg College.

Printing:

Unnecessary printing is wasteful in cost and materials and conflicts with Gettysburg College's sustainability goals. Users are expected to use network printing in a responsible manner by printing only those materials essential to educational, academic, or College needs and by printing selected text rather than full text when possible. Gettysburg College reserves the right to limit, restrict, revoke, or modify any User's individual printing rights and permissions at any time if Gettysburg College determines, in its sole discretion, that the User has abused their access to printing resources or used printing resources in a manner that violates this Network User Policy or any other policy of Gettysburg College.

Business Transactions/Personal Use:

The conduct of occasional private business or financial transactions when such uses are de minimus and sporadic in nature is permitted, provided such use does not degrade the Network's performance, negatively impact others' ability to access and utilize the Network for their purposes, or otherwise conflict with any other Gettysburg College policies.

Remote Server Services:

Approval from the Chief Information Officer is required before any User may install or use any remote access software or any server software on any computer or device connected to the Network.

Equipment and Configuration Control:

Without specific authorization, Users of the Network or College-owned equipment, devices, or facilities must not maliciously cause, permit, or attempt any destruction, modification, deletion, or removal of any data, record, or communications stored on the Network. In addition, the malicious destruction, modification, removal or attempted removal of College-owned equipment, devices, documents or records is prohibited and will be considered a violation of the employee or Community Standards and may result in disciplinary action. Without specific written authorization from the Information Technology Department, Users must not physically or electronically attach any unauthorized device to the Network or to any Gettysburg College owned equipment or device.

Personally-Owned Devices:

When a User attaches any personally-owned device to the Network, the User assumes all risk and liability to and for the use of that device, including but not limited to total loss of any data on the device and the device itself. Personally owned devices and storage media may not be backed up on the Network, Systems, or hardware.

No personally owned device may cause degradation or impairment to any System, hardware, software, or other resource which is part of, or used in conjunction with, the Network. The Information Technology Department is the sole judge of degradation and/or impairment.

Other than for the purpose of supporting currently enrolled students with the devices they own and for supporting Users in configuring Multi Factor Authentication (MFA), the Information Technology Department will not install, uninstall, or assist with the hardware or software configuration of any personally owned device.

The Information Technology Department will seek compensation for damages or disruption of services caused by, or the result of, any use of a personally owned device.

Personal devices used to access College Networks or Data must comply with security requirements established by Information Technology. The College reserves the right to require security software, configuration settings, or other measures on personal devices that access College resources.

Any use of a personally - owned device that constitutes a violation of this policy may also be considered a violation of the student Community Standards or employee Code of Conduct.

Authorized College Staff may make appropriate changes to any computer or device connected to the Network consistent with this Network Use Policy, or when necessary for maintenance, repair, or to protect the Users.

Prohibited Activities

Spreading Computer Viruses and Malware: Deliberate attempts to degrade or disrupt the performance of the Network, any devices connected to the Network, or any other computer System or network on the Internet by spreading computer viruses, worms, malware or other similar programs may be criminal activity under Federal, state, and local law, and is specifically prohibited by this policy.

Impersonation:

Impersonation, false representation, forgery, use of pseudonyms, spoofing, deception, and other methods of hiding or cloaking the true identity of an individual or User in order to mislead or avoid detection is prohibited. The creation, alteration, or deletion of any electronic information contained in or posted to any computer, device, System or other Network resource for any malicious, fraudulent or deceptive purpose is prohibited. Gaining or attempting to gain unauthorized access to, or to make unauthorized use of, accounts, files, records, equipment, electronic resources, or networks is prohibited. Violating the privacy of others is also prohibited.

Business Transactions:

The use of the Network and/or personal web pages to offer goods or services of a business or commercial nature is not permitted, except when consistent with the College's educational or business mission and with the prior written authorization of the Chief Information Officer.

Illegal Activities:

Use of the Network for any activity contrary to federal, state, or local laws is prohibited. Illegal activities include, but are not limited to, tampering with computer hardware or software, unauthorized entry into computer systems or computer data, willful vandalism or destruction of computer data or files, or any attempt to defeat the Network security systems. All Users are expected to abide by the Information Management Policy, the Acceptable Use Policy and all other Gettysburg College policies.

Expectations of Privacy

Gettysburg College endeavors to afford reasonable privacy for Users of the Network and Systems and does not access information created and/or stored by users except when there is a legitimate operational need to do so. Therefore, Users of the Network and Systems are advised that Gettysburg College may access information and data, including personal content. This may include, without limitation, the monitoring, interception, blocking, deleting, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings, logs, browsing data, and other uses of devices and Systems.

Gettysburg College may, in its sole discretion, store copies of such data and communications for a period of time after they are created and may delete such copies from time to time without notice and without liability to the User. Any expectation of privacy is

subject to the terms of the Gettysburg College Access to Electronic Information Policy.

Policy Management

Violations and Sanctions

Reporting Violations:

Users should and are encouraged to report any knowledge or evidence of violations of the Network Use Policy to the Chief Information Officer. Incidents of harassment must be reported in accordance with the Student, Faculty, and Employee handbooks.

Penalties:

Any User who fails to complete required security training in a timely manner will have their Network access temporarily revoked.

Students who violate the Network Use Policy may be subject to the full range of sanctions set forth in the Student Handbook, suspension or termination of Network privileges, and/or other appropriate disciplinary action.

Other Users who violate this policy may be subject to sanctions set forth in the Employee Standards of Conduct and/or Network Use limitations or restrictions, as determined by the Chief Information Officer, Provost, Office of Human Resources, or other appropriate College official.

Information Technology has the authority to temporarily revoke Network access or take other appropriate action in order to maintain Network security or integrity with no prior warning.

This policy will be reviewed every three years and updated as needed.

Related Materials

- Gettysburg College Mission Statement
- Gettysburg College Freedom of Expression Philosophy
- Gettysburg College Ethics and Integrity Program
- Gettysburg College Access to Electronic Information Policy
- Information Management Policy