

[This policy was approved by the Student Life Council and the President's Council and became effective April 26, 2001. See revision history below.]

Gettysburg College Computer Network Use Policy

Introduction: Gettysburg College provides a campus computer network, including access to the Internet (the "Gettysburg College Network"), for students, faculty, administrators, staff, alumni, parents, and friends of Gettysburg College in order to further the educational purposes of the College.

Use of the Gettysburg College Network 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.

College Authority: By using the Gettysburg College Network, users are granting permission for authorized Gettysburg College personnel to monitor, review, and/or intercept electronic communications, electronic records and data, and user information (as further defined below). Access that is necessary to render services or to protect the property of the provider of the service is allowed under the Electronic Communications Privacy Act of 1986 (ECPA). Further, electronic mail and other forms of electronic communication (E-mail) are neither secure nor protected by the laws that apply to the United States Postal Service. E-mail, records, files, communications, generated meta data, voice mail, text messages, social media activity, and any other network activity created using, stored on, generated on, transmitted via, or received by the Gettysburg College Network are Gettysburg College property and are subject to review by authorized personnel designated by Gettysburg College.

Privileges of Network Users

Privacy: As you use our network services we collect certain information about you and the services you use. The information we collect falls into two different categories: (1) information you give us; and (2) information we collect from you automatically when you use our services.

Information You Give Us: We collect information you give us when you use our services. The information you give us may include your first or last name, username, password, email address, postal address, phone number, demographics information, and any other information you choose to give us.

Information We Collect When You Use Our Services: When you use our services or install a Gettysburg College mobile application; or use a computer, tablet, smart phone, or other device on or near the Gettysburg College Network; or access our website we may collect information about the device that you use and how you use it. This user information may include the type of device, your operating system, your web browser, your internet protocol address, your device identifier, information about your physical location, the date and time that you accessed our service, and the web pages you accessed.

How We Use the Information We Collect: We may use the aggregated information we collect about users in a variety of ways, including but not limited to communicating with you; responding to your service inquiries and requests for information; offering you personalized content, products, events, or other promotional purposes; maintaining and improving our business processes or systems; maintaining and improving your experiences with Gettysburg College; detecting, preventing, or investigating security breaches or fraud; enforcing our agreements or policies; and maintaining appropriate records for internal administrative purposes.

How We Share Information: We may disclose your personal information internally or to a third party if we believe that the disclosure is required by law, if we believe that the disclosure is necessary to enforce our agreements or policies, or if we believe that the disclosure will help us protect the rights, property, or safety of Gettysburg College students, employees, and/or visitors.

The College reserves the right to gain access to otherwise private Gettysburg College Network correspondence or files maintained on Gettysburg College Network. System administrators may also require access to otherwise private communications or files maintained on the Gettysburg College Network as part of regular system maintenance. An attempt will be made to notify the user of this access in advance whenever possible and appropriate. Such access is governed by applicable Federal, state, and local laws.

Access: The primary purpose of the Gettysburg College Network is to support academic endeavors. This priority is followed by the College's business requirements. Beyond these primary functions, all users of the Gettysburg College Network will generally be granted equitable access to network resources and services as technology and network capacities allow.

Intellectual Freedom: Gettysburg College encourages a free and open forum for personal expression. This includes viewpoints that are unorthodox or unpopular. Except for official statements from appropriate College officers, Gettysburg College does not officially endorse any opinions stated on the Gettysburg College Network.

Protection from Harassment: All users are encouraged to communicate differing perspectives. Community members are also, however, entitled to work and live in an environment free of harassment. Therefore, any Gettysburg College Network activity that violates the College's harassment policies as defined at the [Gettysburg College Ethics and Integrity Program and Statement of Ethical Behavior](#) web page is prohibited. Defamatory remarks and obscenity are also prohibited. The use of overt profanity is strongly discouraged. Use of the Gettysburg College Network must comply with applicable Federal, state and local laws.

Responsibilities of Network Users

Account Responsibility: Access to the Gettysburg College Network is through individual accounts with password protection. Accounts and passwords are not to be shared. All violations of this policy that can be traced to an individual account name 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 will not be allowed. Electronic chain letters, mail bombs, malware, spamming and excessive recreational use of the Gettysburg College Network are prohibited.

Copyrights: Network 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 the licenses. Upon request from a network administrator, individuals who have software licensed to them and installed on a Gettysburg College computer shall produce original disks and/or documentation to verify compliance.

Printing: Network 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.

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 Gettysburg College Network performance.

Remote Server Services: Approval from the Vice President for Information Technology is required before any member of the Gettysburg College user community may install or use any remote access software or any server software on any computer connected to the Gettysburg College Network.

Equipment and Configuration Control: Without specific authorization, users of the Gettysburg College 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 Gettysburg College Network. In addition, the malicious destruction, modification, removal or attempted removal of College owned equipment, devices, documents or records is prohibited.

Without specific written authorization from the Information Technology Division, users must not physically or electronically attach any unauthorized device to the Gettysburg College Network or to any Gettysburg College owned equipment or device. Authorized devices are limited to the items listed on the [Information Technology Approved Device List](#) web page.

A Note on Personally Owned Devices:

- When you attach any personally owned device identified in the [Information Technology Approved Device List](#) web page, you assume all risk, including but not limited to total loss of your data and personally owned device. Personally owned devices and storage media MAY NOT be backed up on the Gettysburg College Network, systems, or hardware.
- No personally owned device as defined in the [Information Technology Approved Device List](#) web page may cause degradation or impairment to any system, hardware or software which is part of, or used in conjunction with, the Gettysburg College

Network. The Information Technology Division is the sole judge of degradation and/or impairment.

- The Information Technology Division will not install, uninstall, or assist with the hardware or software configuration of any personally owned device.
- The Information Technology Division will seek compensation for damages or services caused by, or the result of, any use of a personally owned device.

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

Prohibited Activities

Spreading Computer Viruses and Worms: Deliberate attempts to degrade or disrupt the system performance of the Gettysburg College Network or any other computer system or network on the Internet by spreading computer viruses, worms, malware or similar programs may be criminal activity under Federal, state and local law, and is specifically prohibited by this policy. As a precondition for network attachment and use, all personal computers and devices capable of running antivirus software must have up-to-date virus protection software installed and operating.

Impersonation: Impersonation, false representation, forgery, pseudonyms, spoofing, deception, and other methods of hiding or cloaking the true identity of a user in order to mislead or avoid detection is prohibited. Gaining or attempting to gain unauthorized access to, or make unauthorized use of, accounts, files, records, equipment or networks is prohibited. Violating the privacy of others is also prohibited.

Business Transactions: The use of the Gettysburg College Network and/or personal web pages to offer goods or services of a business or commercial nature is not permitted except those consistent with the College's educational or business mission.

Illegal Activities: Use of the Gettysburg College 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 Gettysburg College Network security systems. All users are expected to abide by the [Information Management Policy](#) and the other Gettysburg College policies as list on the [Gettysburg College Ethics and Integrity Program and Statement of Ethical Behavior](#) web page.

Violations and Sanctions

Reporting Violations: Users should report any knowledge or evidence of violations of the Network Use Policy to the Vice President for Information Technology or the Vice President for

College Life. Incidents of harassment must be reported in accordance with the Student, Faculty, and Employee handbooks.

Process: Reported violations will be investigated. If the investigation yields evidence of a violation of the Network Use Policy, the case will be heard through the normal College processes for reviewing a violation of policy. For example, possible violations involving students would be heard through the Student Judicial System; those involving faculty members, through the Office of the Provost; and those involving other members of the College community, through the Department of Human Resources.

Penalties: Students who violate the Network Use Policy may be subject to the full range of sanctions as set forth in the Judicial System section of the Student Handbook, including, but not limited to, possible suspension or termination of network privileges.

Other users who violate this policy will be subject to sanctions and/or network use limitations as determined by the Provost, Director 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 health until the Vice President for College Life (or other designee) reviews an alleged infraction of the Network Use Policy.

Revision history

9/20/2001 by mbh. Revised language to change Information Resources to Information Technology. Reformatted line lengths. Added bolding.

[Revised on 4/11/2008] Equipment and Configuration Control revised to permit selected, personally owned devices. Remote Server Services and Reporting Violations language revised from Vice Provost for Information Technology to Vice President of Information Technology.

Revised Equipment and Configuration Control on 12/18/2009 to reword devices permitted on the network.

[revised on 6/23/2011] Equipment and Configuration Control revised to include tablets. Minor wording changes for clarity and flexibility.

[revised on 6/23/2015] Modified most sections of the policy. Added sections: Information You Give Us, Information We Collect When You Use Our Services, How We Use the Information We Collect, How We Share Information. Moved Approved Device List to a web page.