

# Computer Network Use Policy

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

## I. Introduction

Gettysburg College provides a campus computer network, including access to the Internet (the "Gettysburg College Network" or the "Network"), in order to further the educational purposes of the College.

### Network Use Policy

#### Access to Electronic Information Policy

**Scope:** Use of the Gettysburg College Network by students, faculty, administrators, staff, alumni, parents, and friends of Gettysburg College ("Network Users," collectively) 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.

## II. Privileges of Network Users

**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 may include 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.

The Gettysburg College Network and other digital resources may not be used to 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 any images, sounds, or messages 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 inappropriate images, sounds, or messages that are or are intending to be threatening, hostile, or harassing in contradiction to the Gettysburg College Community Standards and Conduct Procedures. 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, or any other behavior in conflict with Gettysburg College policy will be considered a violation of the Community Standards.

Use of the Gettysburg College Network must comply with applicable Federal, state, and local laws.

### **III. 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. You should make a reasonable effort to protect your passwords and other credentials and to secure resources against unauthorized use or access. You must configure your hardware and software in a way that reasonably prevents unauthorized users from accessing the Gettysburg College Network and other resources using your credentials. You are individually responsible for the appropriate use of all digital resources assigned or allocated to you; therefore, you are accountable to Gettysburg College for all use of such resources. 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. Use of the Gettysburg College Network to transmit electronic chain letters, mail bombs, malware, viruses, or spam is prohibited. Gettysburg College may choose to set limits on an individual's use of resources through quotas, time limits, and other mechanisms to ensure that the Network and its resources will be available to and can be used by those who need them.

**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. The installation, activation, and/or use of unlicensed software, or the use of software in a manner that exceeds the scope of the any license, is prohibited within the Gettysburg College 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. 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 or otherwise conflict with any other Gettysburg College policies.

**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 and will be considered a violation of the Community Standards and may result in disciplinary action.

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.
- ▮ Any use of a personally owned device that constitutes a violation of this policy may be considered a violation of the Community Standards and may subject the owner and user of that device to disciplinary action.

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 and/or Network Users.

## **IV. Prohibited Activities**

**Spreading Computer Viruses and Malware:** Deliberate attempts to degrade or disrupt the system performance of the Gettysburg College Network, any devices connected to the Gettysburg College 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. 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. The creation, alteration, or deletion of any electronic information contained in or posted to any computer, device, system or other Gettysburg College Network resource for any fraudulent or deceptive purpose 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 listed on the Gettysburg College Ethics and Integrity Program and Statement of Ethical Behavior web page.

## **IV. Expectations of Privacy**

Gettysburg College endeavors to afford reasonable privacy for users of the Gettysburg College 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 Gettysburg College Network and systems are advised that Gettysburg College may access information and data, including personal content. This may include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings, and other uses of devices and systems. Gettysburg College may also 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. Any expectation of privacy is subject to the terms of the Gettysburg College Access to Electronic Information Policy.

## **V. 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.

**Penalties:** Students who violate the Network Use Policy may be subject to the full range of sanctions as set forth in the Community Standards Sanctioning guide of the Student Handbook, including, but not limited to, possible suspension or termination of network privileges, in addition to other appropriate disciplinary action.

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.