Purpose

This policy describes the appropriate uses of computers, networks, hardware and software at Hamilton College. In addition, it describes responsibilities of individuals and Hamilton College with respect to the confidentiality and privacy of information stored on institutional computers.

Scope

This policy applies to all individuals using Hamilton College's computers, networks and related hardware and software.

Policy Revision History

Last revised, December 2014.

Table of Contents

- Individual Responsibility
- User IDs and Passwords
- Protecting Desktop Equipment and Files
- Confidentiality and Privacy
- Institutional Privileges
- Legal Compliance
- Indemnification
- Inappropriate Uses - Examples
- Noncompliance and Sanctions

Hamilton College is a private institution fully committed to the ideals of academic freedom, freedom of expression, and cultural diversity. Inappropriate behavior and malicious misuse of information technology resources that in any way degrades the College equipment and services or violates the rights of others in the community is strictly prohibited.

Individual Responsibility

While LITS is responsible for monitoring the use of computer systems, it is the responsibility of all individuals in the Hamilton community use information technology resources in accordance with this policy. Each member of the community is responsible for using only those accounts or computers for which he or she has authorization and is responsible for protecting all passwords.
Individual responsibility includes respecting the rights of other users. Individuals are urged to report unauthorized use of computers, networks, or other LITS facilities on campus by calling the LITS Help Desk or notifying the Vice President for Libraries and Information Technology.

**User IDs and Passwords**

Access to information technology resources is provided via user ID and password system. Users are personally responsible for the security of the ID and password assigned to them. Viewing, copying, altering or destroying any file, or connecting to a computer on the network without explicit permission of the owner is prohibited.

Passwords should be known only to the person responsible for the account and user ID. Access to user IDs may not be loaned or sold and any suspected breach of password security should be immediately reported to the LITS Help Desk. Passwords should be changed (at least) every twelve months by employees and students.

**Protecting Desktop Equipment and Files**

Backups and protection of files stored on desktop equipment are the responsibility of the user of that equipment. Users must back up their work files on a regular basis. LITS licenses Crashplan software for this purpose. Additionally, LITS provides central electronic storage for employees and students. This storage is backed up daily and backups are generally available for a period of six months.

Individual users are responsible for safeguarding the equipment entrusted to them by the college. This includes reasonable protection of equipment from damage and theft.

**Confidentiality and Privacy**

Hamilton takes reasonable steps to protect users from unauthorized entry into their accounts or files, whether by other users or by system administrators, except in instances where a system-related problem requires such entry. A limited number of authorized Hamilton personnel must occasionally monitor information on the network and/or computer systems to maintain the integrity of the systems. This access is required for reasons that include, but are not limited to, trouble-shooting hardware and software problems; preventing unauthorized access and system misuse; providing for the overall efficiency and integrity of the systems; protecting the rights and property of the College; ensuring compliance with software and copyright, distribution, assuring that computer systems meet college requirements for virus protection and operating system updates before connecting to the campus network, and other College policies concerning the use of the computer network; and complying with legal and regulatory requests for information.

System monitoring is a mechanism for keeping track of computer system activities, rather than a method for accessing private information. LITS personnel also take reasonable steps to prevent the dissemination of information concerning individual user activities. It is the policy of LITS to disclose neither the contents of electronic mail and data files stored in or transmitted via the College information technology resources, nor the activities of individuals on the campus network, to other individuals within or outside the College community except when required to do so by law, legal mandate, during legal investigations (in accordance with College policies) or by permission of the owner. In addition, the College assumes ownership of the employee’s account(s) from the time access is terminated until the account(s) is/are deleted. If it is necessary to ensure business continuity, designated personnel may be granted access to the account(s) during this period.
Private communication via computer is treated with the same degree of protection as private communication in other media. However, due to limits of current technologies, which are inadequate to protect against unauthorized access, the confidentiality of e-mail and other system files cannot be assured. All users should be aware of this and use reasonable caution when transmitting confidential materials.

Access to computer operations areas is restricted to those responsible for operation and maintenance. Computing facilities on campus are secured when not open for business. LITS takes action to provide reasonable protection against environmental threats such as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power for server and network facilities. LITS maintains procedures for protecting critical data that reside on central servers. While Hamilton provides security for files stored on central computing facilities, Hamilton cannot be responsible for protection against floods, fires, and catastrophic events of this type. LITS does not guarantee the availability of backups for the restoration of files deleted through user error.

Institutional Privileges

Hamilton College reserves the right to allocate information technology resources. To accomplish this, the system administrators may suspend or terminate privileges of individuals without notice if malicious misuse or use inconsistent with this policy, any other College policy, or applicable law is discovered. Privileges may also be suspended, without notice, to meet time-dependent, critical operational needs.

Legal Compliance

All existing federal and state laws and College regulations and policies apply to the use of computing resources and all users of such resources are required to be in compliance with all laws, regulations and policies at all times. This includes not only those laws and regulations that are specific to computers and networks, but also those that apply generally to personal conduct. As such, any of these resources may be subject to review by designated College personnel in accordance with College policies.

Indemnification

Users agree, in consideration of access to the College's information technology resources, to indemnify, defend, and hold harmless the College for any suits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the College's computing, networking, and media services and facilities.

Inappropriate Uses - Examples

The following are examples of violations of information technology resources policies at Hamilton College.

- **Malicious misuse.** Using IDs or passwords assigned to others, disrupting the network, destroying information, removing software from public computers, spreading viruses, sending e-mail that threatens or harasses other people, invading the privacy of others, and subscribing others to mailing lists or providing the e-mail addresses of others to bulk mailers without their approval.
- **Unacceptable use of software and hardware.** Knowingly or carelessly running or installing unlicensed software on any computer system or network; giving another user a program
intended to damage the system; running or installing any program that places an excessive load on a computer system or network, or compromises the security of the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.

- **Inappropriate access.** Unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus network to gain unauthorized access to any computer system; connecting unauthorized equipment to the campus network including wireless access points; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data); knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks; deliberately wasting or overloading computing resources, such as printing too many copies of a document; or other activities.

- **Inappropriate use of electronic mail and Internet access.** Initiating or propagating electronic chain letters; inappropriate mass mailing including multiple mailings to newsgroups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication or sending anonymous e-mail; using another person's e-mail account or identity to send e-mail messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; or using e-mail or personal web page advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.

**Noncompliance and Sanctions**

LITS may suspend or terminate all computing privileges of any individuals without notice who engage in improper computing activities. Serious cases, as determined by the Vice President for Libraries and Information Technology, may result in disciplinary action against the individual including the suspension, expulsion, or termination of the offending individual, as appropriate and as determined at the sole discretion of Hamilton College. Where violation of state and federal law is involved, cases will be referred to the proper legal authorities for action.

[Return to Policies](#)

_Last Updated: April 1, 2015_