Hamilton

Appropriate Use of Information Technology Resources

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.

Contents

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.

All use of IT resources must comply with:

- all College policies, procedures, and codes of conduct, including those found in the student, faculty, and employee handbooks;
- all laws and regulations applicable to the user or the College; and
- all relevant licenses and other contractual commitments of the College, as modified from time to time.

Individual Responsibility

While LITS is responsible for monitoring the use of computer systems, it is the responsibility of all individuals in the Hamilton community to 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. Users are personally responsible for the security of the credentials assigned to them.

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

Viewing, copying, altering or destroying any file, or connecting to a computer on the network without the explicit permission of the owner is prohibited.

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 employees 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:

- troubleshooting 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;
- other College policies concerning the use of the computer network;

- 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:

1. when required to do so by court order/ subpoena;
2. during investigations related to violations of College policies;
3. in health and safety emergencies;
4. when the user of the account is unavailable for an extended period, and the information contained in the account is necessary to conduct college business;
5. when the user of the account leaves the College;
6. when the user of the account dies;
7. by permission of the account holder.

Procedures for dealing with exceptions (1-6 above):

Court Order/ Subpoena

Hamilton may be under legal obligation to respond to court orders/subpoenas by producing information stored in electronic accounts. If Hamilton receives a court order/subpoena, the VP for Libraries and IT will consult with Hamilton's attorneys,

as necessary, and appoint a LITS member to assist in collecting the data as required in the court order/subpoena. The appointed LIST member will be required to treat this data with strict confidentiality.

Investigations of Violation of College Policies

Requests for access to user accounts in connection with investigations of alleged violations of College policies must be made by a member of Senior Staff to the Director of Human Resources (for employees) or Dean of Students (for students). After receiving such a request, the Director of Human Resources or Dean of Students will consult with Hamilton's attorneys as necessary to determine if the College needs to preserve the electronic content of those involved for further investigation. Upon request from the Director of Human Resources or Dean of Students, the VP for Libraries and IT will appoint a LITS member to assist in collecting the data as required. The appointed LITS member will be required to treat this data with strict confidentiality.

Health and Safety Emergencies

In the event of a health and safety emergency, it may be necessary to access or disclose electronic content to local, state, or federal emergency responders, or to officials involved with an emergency response at the College. A request for information must come from a member of Senior Staff (other than the VP for Libraries and IT). Upon receipt of a request, the VP for Libraries and IT will appoint a LITS member to assist in collecting the data as needed. The appointed LITS member will be required to treat this data with strict confidentiality.

User of the Account is Unavailable for an Extended Period of Time

There are situations in which employees may take an extended leave of absence from the College. In planned absences, employees are expected to place an out-of-office message on the email account directing people who to contact in their

absence. For unplanned extended absences, it may be necessary for the College to access incoming mail for continuity of business operations. In these instances, a request will be made by the member of Senior Staff who heads the division in which the employee resides to the VP for Libraries and IT, who will appoint a LITS member to assist in collecting the data as needed. The appointed LITS member will be required to treat this data with strict confidentiality.

When the User of the Account Leaves the College

The College maintains ownership of the employee's account(s) from the time access is terminated until the account(s) is/are deleted. Procedures for termination of accounts are described in the Access to Information Technology Resources policy (https://my.hamilton.edu/lits/rc/policies-access-to-information-technology-resources).

When the User of the Account Dies

The personal representative of the estate of the deceased may request access to the user's electronic content for a period of one year following the death for the purpose of gathering personal materials of the deceased. The request should be made to the VP for Libraries and IT, accompanied by a legal document that indicates the status of the requestor and the nature of information being requested (such as an order of the Surrogate's Court appointing the requester to act as executor). These requests will be handled in consultation with the College's attorneys. The VP for Libraries and IT will appoint a LITS member to assist in collecting the data as needed. The LITS member will be required to treat this data with strict confidentiality.

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 is 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 the college harmless 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 email that threatens or harasses other people, invading the privacy of others, and subscribing others to mailing lists or providing the email 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 email; using another person's email account or identity to send email 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.

The above examples are only meant to provide general guidance and are by no means exhaustive.

Noncompliance and Sanctions

Users who violate this policy may be denied access to the institution's resources and may be subject to penalties and disciplinary action, both within and outside the institution, subject to the appropriate enforcement process. The institution may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect the institution from liability.

198 College Hill Rd, Clinton, NY 13323

315-859-4011