RESPONSIBLE USE OF COMPUTING RESOURCES AT MOUNT HOLYOKE COLLEGE

Summary

The College has adopted this policy on Responsible Use of Computing Resources at Mount Holyoke College to provide guidance to members of the community. This policy has been incorporated into Faculty Legislation and the Staff and Student Handbooks.

The document provides that all users of campus computing resources must:

- Comply with all federal, state and other applicable law, all applicable College rules and policies and all applicable contracts and licenses.
- Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.
- Respect the finite capacity of College resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.
- Refrain from using those resources for personal commercial purposes or personal financial or other gain not related to the mission of the College.
- Refrain from stating or implying that they speak on behalf of the College and from using College trademarks and logos without authorization to do so.
- Be attentive to computer problems than may be the result of worms, viruses, spyware, keystroke loggers or other invasive software.

Introduction

As a part of the institution's physical facilities and academic and social infrastructure, Mount Holyoke College acquires, develops and maintains computers, computer systems and networks. These resources are owned by the College and intended for College related purposes, including direct and indirect support of the College's teaching and research, of administrative functions, of student and campus life activities and of the free exchange of ideas among members of the College community and between the College community and the wider local, national and world communities.

The rights of academic freedom and freedom of expression apply to the use of College computing resources, as do the responsibilities and limitations associated with those rights. The use of College computing resources, like the use of any other College-provided resource or College-related activity, is subject to the normal requirements of legal and ethical behavior within the College community. Legitimate use of a computer, computer system or network does not extend to whatever is technically possible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network, and whether or not they can be circumvented by technical means.

This policy applies to all users of College computing resources, whether affiliated with the College or not, and to all uses of those resources, whether on campus or from remote locations. In addition, once a computer is attached to College systems, College policies apply to its use, regardless of the ownership of the computer. Additional policies may apply to specific computers, computer systems or networks provided or operated by specific departments of the College or to uses within specific departments. For more information, consult the department head or operator of the particular computer, computer system or network.

Policy

All users of College computing resources must:

- **Comply with all federal, state and other applicable law, all applicable College rules and policies and all applicable contracts and licenses.** Examples include the laws of libel, privacy, partisan political activity, copyright, trademark, obscenity and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act (which prohibit "hacking", "cracking" and similar activities); the College's honor code and Statement on Individual Rights and Community Responsibility; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries, on other systems or networks, or who post to web sites that are viewable in other states or countries should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

- **Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.** Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, provided to or used by, persons other than those to whom they have been assigned by the College. Unless specifically authorized by the Director of Networking, computers connected to the College's network should not be used to provide access to internal campus resources to those who would not otherwise have access to them.

- **Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** The ability to access

other persons' accounts does not imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

- **Respect the finite capacity of the College's resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.** Although there is no set bandwidth, disk space, CPU time or other limit applicable to all uses of College computing resources, the College may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

- **Refrain from using those resources for personal commercial purposes or personal financial or other gain not related to the mission of the College.** Personal use of College computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other College responsibilities, and is otherwise in compliance with this policy. Advertising for non-College ventures is not permitted. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

- **Refrain from stating or implying that they speak on behalf of the College and from using College trademarks and logos without authorization to do so**. Affiliation with the College does not imply authorization to speak on its behalf. If it is unclear whether a proposed use of College trademarks and logos is authorized, guidance should be sought from the Office of Communications.

- **Be attentive to computer problems that may be the result of worms, viruses, spyware, keystroke loggers or other invasive software.** A compromised computer puts both the individual machine and the larger system at risk. If you suspect that your computer has been compromised, notify LITS immediately. In addition, be cautious about downloading materials (e.g., P2P software, screen savers, tool bars) that make the computer more vulnerable to outside attack or otherwise interfere with other software on the machine. For more information about appropriate use of P2P software, see the policy on Employee Use of Peer-to-Peer File Sharing Software.

<u>Oversight</u>

The College has created a Privacy/Security Committee to monitor legislation and regulation in this area, develop appropriate institutional policies and communicate with the Mount Holyoke community. The Chair of the Committee is the Vice President for Finance and Administration, who in consultation with the Committee serves as the Chief Security Officer for the College.

<u>Enforcement</u>

Users who violate this policy may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Violations will normally be handled through the College disciplinary procedures applicable to the relevant user. The College may temporarily suspend or block access to an account or restrict network access 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 College or other computing resources or to protect the College from liability. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Security and Privacy

The College employs various measures to protect the security of its computing resources and of users' accounts. Users should be aware, however, that the College cannot guarantee such security. Users should engage in safe computing practices by establishing appropriate access restrictions for their accounts, including appropriate selection and safekeeping of passwords.

Users should also be aware that their uses of College computing resources are not completely private. The normal operation and maintenance of the College's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. Such audits may review the sizes, kinds and names of software and files, but do not review the contents of documents.

While in general content is not reviewed, it is important to understand that all information related to the business of the College is owned by the College. If an account has been closed or expired, or the account owner is not available within a reasonable period of time, the Director of Networking or his/her designee, in consultation with the Director of Human Resources, may move files or provide an authorized supervisor with access.

With the prior authorization of the Director of Networking or the Director's designee, the College may specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when one or more of the following occurs:

- **a.** The user has voluntarily made them accessible to the public, as by posting to a web page.
- **b.** It reasonably appears necessary to do so to protect the integrity, security or functionality of College or other computing resources or to protect the College from liability.
- **c.** In the course of an investigation into possible misconduct or illegal activity.
- **d.** In a situation involving health or safety issues.
- **e.** There is reasonable cause to believe that the user has violated or is violating this or related policies.
- **f.** An account appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns. It is otherwise required or permitted by law.

The College, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to

appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary proceedings. For more information, see the statement on Anonymity in Computer Use.

MHC PRIVACY/SECURITY COMMITTEE
Revised 12/20/10