

Mount Holyoke College Summary of Computer Use Policies

The College has adopted a [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 that may be the result of worms, viruses, spyware, keystroke loggers or other invasive software.

Two issues deserve particular emphasis:

- **Peer-to peer file sharing software.** The use of P2P software on College machines or any machine connected to the College network for purposes other than academic or job-related uses is prohibited. Given the risks of contamination, inadvertent violation of the copyright laws and demand for bandwidth involved, for your own protection and that of the College, faculty or staff members who have legitimate needs for P2P software should consult with the Dean of Faculty or the appropriate division head about your plans to use P2P software and with LITS about the safest way to do so.
- **Safeguarding personal/confidential information.** The news continues to be full of instances in which organizations, many of them colleges and universities, have inadvertently released individuals' personal information and exposed them to the risks of identity theft. Faculty and staff who work with such information should use the campus servers whenever possible so the information does not reside on individual desktop machines. Personal or confidential information

should not be downloaded onto portable devices, such as laptops, PDA's or flash drives.

The complete text of these policies, related policy documents, informational materials and the College's record retention guidelines are available at www.mtholyoke.edu/lits/network/docs/policies/. If you have questions or would like to schedule a training session, please write to privsec-tf@mtholyoke.edu.

8/31/09 MJMaydew