HARTWICK COLLEGE

USER RESPONSIBILITIES AND APPROPRIATE USE POLICY

Hartwick College provides technology resources in support of the College's purpose as a liberal arts and sciences institution, our educational and community values, and our programs and initiatives. Hartwick's Information Technologies organization's goal is to provide high quality services to the College community.

To ensure that our high standards are met, we have certain expectations regarding the use of technology resources at the College. The purpose of this policy is to encourage the responsible use of our technology resources consistent with the College's expectations for the appropriate conduct of the members of its community. As such, it supplements existing College policies. This document is intended to provide guidance to users. It describes activities that Hartwick College considers violations of use of technology resources. The examples listed are not intended to be exhaustive since technology and applications consistently change.

If you are unsure whether any use or action is permitted, please contact the Technology Resources Center at x4357 for assistance.

Access to Hartwick College technology resources is a privilege, not a right. This privilege is extended to all users including faculty, staff, students, trustees, alumni/ae, and affiliated individuals and organizations. Hartwick's technology resources include computing facilities, telecommunications and network services, video network services, web page servers, equipment, software, applications, information resources, printing and scanning services, and user and technical support provided by Information Technology staff. Accepting access to these technology resources carries an associated expectation of responsible and appropriate use.

In General

While there are cases in which use of technology resources is deemed not responsible or not appropriate, there are also cases in which technology resources are used in the conduct of behaviors which violate College policies, codes of conduct, or local, state, or federal laws. Though the use of technology resources is the focus of this document, members of the Hartwick community and others using Hartwick technology resources are advised that use may also be governed by other College policies including but not limited to those in the student handbook, College catalog, employee and faculty handbooks; other policies governing academic, student life, or personnel matters at the College; or agreements between the College and affiliated organizations. Hartwick College's technology and information resources are not to be used for commercial purposes or non-College related activities without written authorization from the officer(s) of the College that have been so designated (contact Technology Resources for further information).

Your Responsibilities

As a user of Hartwick technology resources, you have a shared responsibility with the College technologies staff to maintain the integrity of our systems, services, and information so that high quality services can be provided to everyone. Your responsibilities include:

- To use the College's technology resources responsibly and appropriately, consistently with the mission and purpose of the College, and respecting the rights of other users to system, services, and information access 24 hours/day, 7 days per week.
- To be cooperative in reserved computing facilities, such as classrooms or labs scheduled for use for instruction, testing, or workshops.
- To comply with posted policies governing use of public computing and printing facilities.
- To respect all contractual and license agreements, privacy of information, and the intellectual property of others.
- To comply with College, federal, state, and local regulations regarding access and use of information resources (e.g., College policies regarding the Institutional Information System and dissemination of information outside the campus, Federal Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, codes of professional responsibility, etc.).
- To maintain your own system accounts (to include files, data and processes associated with those accounts); for PC files, data, and processes, this includes taking appropriate action to backup your PC system. (Technologies Resources can assist you in setting up backup procedures).
- To exercise due diligence in protecting any computer you connect to the Hartwick network from viruses, worms, and security vulnerabilities by regularly using anti-virus software (provided by Technology Resources for College

issued computers or personally purchased anti-virus software for personally owned computers), installing available security updates/patches for your operating system and any applications you use, and avoiding the installation of untrusted programs on your computer.

- To keep your technology accounts (computer, network, Blackboard, Datatel, voice/calling card/voice mail) secure. If you suspect unauthorized access, report it to your supervisor or the Student Life Office and to Technology Resources, or to the College Security department.
- To not share your privileges with others. Your access to technology resources is not transferable to another member of the Hartwick community, to family members, or to an outside individual or organization. If someone wishes access to Hartwick's technology resources, s/he should contact Technology Resources.
- To present web pages and blogs that reflects the highest standards of quality and responsibility. As page or blog owner, you are responsible both for the content of your web page or blog and that all links and references from these are consistent with this and other College policies, copyright laws, and applicable local, state, federal laws. College-hosted web pages and blogs are not to be used for commercial purposes or for activities not related to the purposes of the College, without written authorization from the College.
- To contribute information to College wikis that reflect the highest standards of quality, accuracy, and responsibility.
- To understand the implications of sharing personal information or data via the Internet, WWW, e-mail, Instant Messaging, or other services that either are open to access by others on and off-campus, or that can be forwarded to others.
- To record your name and an appropriate greeting on your voice mail account.
- To report violations or suspected violations of this policy to Campus Safety or Technology Resources.

Examples of Violations of Appropriate Use

Authorized Access/Accounts

- Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account ("cracking"). This includes accessing data not intended for the user, logging into a server or account you are not expressly authorized to access, or probing the security of systems or networks.
- Supplying or attempting to supply false or misleading information or identification in order to access Hartwick's technology resources.
- Sharing your passwords or authorization codes with others (computing, e-mail, voice mail, long distance code, etc.).
- Using technology resources for unauthorized uses.
- Logging onto another user's account; sending e-mail, voice mail, etc. from another individual's or from an anonymous account.
- Unauthorized use of the College's registered Internet domain name(s).
- Using another person's telephone authorization code, line, calling card, or network system access for chargeable services.
- Using voice services to incur charges for collect or third-party calls which are billed to the College and not to your direct line.
- Changing your Hartwick College-issued machine name to a name that is different from that assigned by Technologies Resources without authorization.
- Connecting computers or other devices to the College network that have not been registered with, or approved by, Technology Resources.

Services

- Attempting to interfere with service to any user, host, or network. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service, port scans and attempts to "crash" a host.
- Use of any kind of program/script/command designed to interfere with a user's computer or network session or collect, use or distribute another user's personal information (spyware).
- Damaging a computer or part of a computer or networking or telecommunications system.
- Knowingly spreading computer viruses.
- Modifying the software or hardware configuration of College technology resources, including dismantling computers in the lab for the purposes of connecting a notebook computer to the peripherals.
- Excessive use of technology resources for "frivolous" purposes, such as game playing or downloading of media files. This causes congestion of the network or may otherwise interfere with the work of others, especially those wanting to use public access PCs or network and Internet resources.
- Violating copyright laws.

- "Hacking" on computing and networking systems.
- Using College technology resources (networks, central computing systems, public access systems, voice and video systems) for new technologies research and development without College review and authorization.
- Failure to follow the College's guidelines for use and/or deployment of wireless access points (WAPs) (click here for the policy document).

Software, Data & Information

- Inspecting, modifying, distributing, or copying software or data without proper authorization, or attempting to do so.
- Violating software licensing provisions.
- Installing software on public access and other College machines without appropriate authorization (from Technologies Resources or the department to which the machines belong).
- Installing any diagnostic, analyzer, "sniffer," keystroke/data capture software or devices on College technology resources.
- Breaching confidentiality agreements for software and applications; breaching confidentiality provisions for institutional or individual information.

Email/Internet Messaging/Voice Mail/Voice Services

- Harassment or annoyance of others, whether through language, frequency or size of messages, or number and frequency of telephone calls.
- Sending e-mail or voice mail to any person who does not wish to receive it, or with whom you have no legitimate reason to communicate. If a recipient asks to stop receiving mail from you, you must not send that person any further mail.
- Sending unsolicited bulk mail messages ("junk mail" or "spam") which, in the College's judgment, is disruptive to system resources or generates a significant number of user complaints. This includes bulk mailing of commercial advertising, informational announcements, political tracts, or other inappropriate use of system e-mail distribution lists. Click here for the College's policy on system distribution messages. Forwarding or otherwise propagating chain e-mail and voice mail and pyramid schemes, whether or not the recipients wish to receive such mailings. This includes chain e-mail for charitable or socially responsible causes.
- Malicious e-mail or voice mail, such as "mailbombing" or flooding a user or site with very large or numerous items of e-mail or voice mail.
- Forging of e-mail header or voice mail envelope information.
- Forging e-mail from another's account. Sending malicious, harassing, or otherwise inappropriate voice mail from another's voice line.
- Collecting replies to messages sent from another institution, organization, or Internet Service Provider where those messages violate this Appropriate Use Policy or the Appropriate Use Policy of that other provider.

College-hosted Web Pages, Blogs, Wikis & Servers

- Posting content on your web page, blog, or wiki that provides information on and encourages illegal activity, or is harassing and defaming to others.
- Linking your web page, blog, or wiki to sites whose content violates College policies, local, state, and/or federal laws and regulations.
- Running websites, blogs, or wikis that support commercial activities or running server systems under the College's registered domain name, HARTWICK.EDU or variation thereof, without the College's authorization. Contact the Technologies Resources Center, 607-431-4357, if you have questions about authorization or wish to apply for authorization.

College Listservs, Bulletin & Discussion Boards

- Posting a message whose subject or content is considered unrelated to the subject matter of the listserv, bulletin or discussion board to which it is posted. For moderated listservs, the decision as to whether a post is unrelated will be made by the moderator. For listservs that are not moderated and discussion boards, we employ the practice of "self-policing" -- that is, members serve as moderators, commenting (to the sender, to the list) about inappropriate posts.
- Posting chain letters of any type.
- Forging header information on posts to College listservs, bulletin or discussion boards.

Enforcement of this Policy

Hartwick College reserves the right to monitor the College's network and systems attached to it, and to take actions to protect the security of the College's systems, information, and users.

Reporting Violations or Suspected Violations

Reports of violations or suspected violations should be made to Campus Safety or Technology Resources.

Response to Violations

Campus Safety and Information Technology will investigate and respond to reports of violations or suspected violations. As part of this response, Information Technology reserves the right to immediately disconnect any system or terminate user access.

Sanctions

The College will enforce applicable penalties and/or immediately terminate access to College systems and network services to any user in cases where technology resources have been used in a manner that is disruptive or is otherwise believed to be in violation of this policy or other College policies or law. As a recognized agent under the Digital Millennium Copyright Act, the College will act in accord with the provisions of this act in the event of notification of alleged copyright infringement by any user.

Instances of inappropriate use of technology resources will be referred to the appropriate official for disciplinary action by the College and will be subject to this policy as well as to other applicable College policies and guidelines. In addition, individuals may be subject to civil suit, and/or local, state, and federal prosecution depending on their actions. Among sanctions that can be imposed for violation of this or other applicable College policies, the College reserves the right to restrict an individual's access to technology resources. The College's Information Technologies Division reserves the right to deny employment within the division to any individual found in violation of this policy. Academic departments reserve the right to not admit to or dismiss students from their programs as a sanction for violation of this policy.

08-14-07 rev.

Signature: _____

Date: _____