

COMMUNITY COLLEGE SYSTEM OF NEW HAMPSHIRE

Section: 300 – Human Resources	Subject: 320 Employment
Policy: Information Technology Acceptable Use	Date Approved: June 16, 2009
Policy #: 321.01	Date of Last Amendment: August 11, 2009
Approved: Richard A. Gustafson, Chancellor Effective Date: July 1, 2009	

321.01 INFORMATION TECHNOLOGY ACCEPTABLE USE

1. Purpose:

The purpose of this policy is to encourage the responsible use of CCSNH and member campus technology resources consistent with expectations for the appropriate conduct of the members of our campus communities. This policy is intended to provide guidance to CCSNH technology users. While this policy and Addendum-A (Examples of Violations) are intended to provide guidance, it is impossible to contemplate all potential applications since technology and applications consistently change. If unsure whether any use or action would constitute a violation of this policy, contact your campus Information Technology department or the System Office for assistance. In cases not covered explicitly by the CCSNH Acceptable Use policy, the System Office determination will prevail. In addition to this policy, information on how to use CCSNH technology, resources and services can be found at www.ccsnh.edu

Access to CCSNH technology resources is a privilege, not a right. This privilege is extended to all users including faculty, staff, students, alumni/ae, and affiliated individuals and organizations. CCSNH'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 acceptable use. Failure to abide by the responsibilities articulated below may result in loss of privileges.

2. Responsibilities

Users of CCSNH technology resources have a shared responsibility with our Information Technology staff to maintain the integrity of our systems, services, and information so that high quality and secure services can be provided to everyone. Toward this end, all users shall:

- a. Comply with posted policies governing use of computing and printing facilities.
- b. Respect all contractual and license agreements, privacy of information, and the intellectual property of others.
- c. Comply with federal, state, and local regulations regarding access and use of information resources (e.g., policies regarding Federal Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, codes of professional conduct and responsibility, etc.).
- d. Maintain and secure your own system accounts (including files and data associated with those accounts); this includes taking action to backup your files and data as appropriate.
- e. Exercise due diligence in protecting any computer you use to connect (either through dial-up, VPN or any other means) to the CCSNH network from viruses, worms, and security vulnerabilities by maintaining and regularly using anti-virus software, installing available security updates/patches for your operating system and any applications you use, and avoiding the installation of un-trusted programs on your computer.
- f. Take precautions to keep your technology accounts (computer, network, Blackboard, Banner, etc.) secure.
- g. Do not share privileges with others. Your access to technology resources is not transferable to other members of the CCSNH community, to family members, or to outside individuals or organizations. If someone wishes access to CCSNH's technology resources, s/he should contact the CCSNH Information Technology Office by sending email to ITSupport@ccsnh.edu
- h. Ensure that any and all of your web pages and blogs reflect 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 for ensuring that all links and references from these are consistent with this and other policies, copyright laws, and applicable local, state, federal laws. CCSNH hosted web pages and blogs are not to be used for commercial purposes or for activities unrelated to the educational mission of the college without written authorization from the CCSNH.
- i. Ensure that any contributions of information to WIKIS reflect the highest standards of quality, accuracy, and responsibility.
- j. Understand the implications of sharing information or data via the Internet, e-mail, Instant Messaging, social networks or other services

that are either open to access by others, or that can be viewed and/or forwarded to others.

- k. Report violations or suspected violations of this policy. Please report violations as follows:
- College Personnel: Report violations to your immediate supervisor, Vice-President of Academic Affairs or President.
 - System Office Personnel: Report violations to your immediate supervisor, Vice-Chancellor or Chancellor.
 - Students: Report violations to your College Vice-President of Academic Affairs or President.
3. Enforcement of this Policy

CCSNH reserves the right to monitor the System network and systems attached to it, and to take actions to protect the security of the CCSNH systems, information, and users.

- a. Reporting Violations or Suspected Violations: Reports of violations or suspected violations as follows:
- College Personnel: Report violations to your immediate supervisor, Vice-President of Academic Affairs or President.
 - System Office Personnel: Report violations to your immediate supervisor, Vice-Chancellor or Chancellor.
 - Students: Report violations to your College Vice-President of Academic Affairs or President.
- b. Response to Violations: The CCSNH Information Technology office will investigate and respond to reports of violations or suspected violations and include appropriate CCSNH offices as necessary. As part of this response, Information Technology reserves the right to immediately disconnect any system or terminate user access to protect the security of the CCSNH systems, information, and users.
- c. Sanctions: Violation of this policy may result in the immediate termination of access and/or disciplinary action by CCSNH including, but not limited to restriction to all CCSNH technology resources and/or denial of employment opportunities with CCSNH. As a recognized agent under the Digital Millennium Copyright Act, CCSNH will act in accord with the provisions of this act in the event of notification of alleged copyright infringement by any user.
- d. Compliance: All users who access or use CCSNH Information Technology resources must agree to comply with the CCSNH Information Technology Acceptable Use Policy. (also referenced in Student Section 730.08)

Addendum A: Example Violations of Acceptable Use Policy

The purpose of this addendum is to provide examples of violations of CCSNH's Acceptable Use Policy. The following is not an exhaustive list and if you are unsure whether any use or action would constitute a violation of this policy, please contact your campus Information Technology department or the System Office for assistance. In cases not covered explicitly by the CCSNH Acceptable Use policy the System Office determination will prevail.

Examples which Apply for ALL Users (Students, Faculty, Staff and Contract Employees):

Authorized Access/Accounts

1. Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account. 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.
2. Supplying or attempting to supply false or misleading information or identification in order to access CCSNH's technology resources.
3. Sharing your passwords or authorization codes with others (computing, e-mail, Blackboard, Banner, etc.).
4. Using technology resources for unauthorized uses.
5. Logging onto another user's account (without the permission of the account owner)
6. Sending e-mail, messages, etc. from another individual's or from an anonymous account.
7. Unauthorized use of CCSNH registered Internet domain name(s).
8. Changing your issued machine name to a name that is different from that assigned by CCSNH or campus Information Technology departments without authorization.
9. Connecting computers or other devices to the CCSNH network that have not been registered with, or approved by, CCSNH.

Services

1. 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.

2. 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.
3. Damaging a computer or part of a computer or networking system.
4. Knowingly spreading computer viruses.
5. Modifying the software or hardware configuration of a CCSNH owned computer with malicious intent
6. Excessive use of technology resources for "frivolous" purposes **unrelated to the academic or administrative work of the Colleges**, Examples are game playing (local or networked), downloading of music/video media files, using peer to peer file sharing programs, listening/watching streaming audio/video feeds (Internet radio, Internet TV, YouTube, etc.). These examples can cause congestion of the campus network and Internet connection or may otherwise interfere with the academic and administrative work of others, especially those wanting to use public access PCs or network and Internet resources.
7. Violating copyright laws.
8. "Hacking" on computing and networking systems.
9. Using technology resources (networks, central computing systems, public access systems, voice and video systems) for new technologies research and development without review and authorization from the CCSNH Information Technology office.
10. Deployment of wireless access points (WAPs) without review and authorization from the CCSNH Information Technology office.

Software, Data & Information

1. Inspecting, modifying, distributing, or copying software or data without proper authorization, or attempting to do so.
2. Violating software licensing provisions.
3. Installing software on public access and other CCSNH owned computers without appropriate authorization from the CCSNH Information Technology office.
4. Installing any diagnostic, analyzer, "sniffer," keystroke/data capture software or devices on CCSNH owned computer equipment or on the CCSNH network.
5. Breaching confidentiality agreements for software and applications; breaching confidentiality provisions for institutional or individual information.

Email/Internet Messaging/Voice Mail/Voice Services

1. Harassment or annoyance of others, whether through language, frequency or size of messages, or number and frequency of telephone calls.
2. 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.
3. Sending unsolicited bulk mail messages ("chain mail", "junk mail" or "spam"). This includes bulk mailing of commercial advertising, informational announcements, political tracts, or other inappropriate use of system e-mail distribution lists. 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.
4. 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.
5. 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 lines.
6. Falsely representing opinions or statements on behalf of CCSNH or others.

CCSNH hosted Web Pages, Blogs, Wikis, Servers and general content

1. Posting content on your web page, blog, or wiki that provides information on and encourages illegal activity, or is harassing and defaming to others.
2. Linking your web page, blog, or wiki to sites whose content violates CCSNH policies, local, state, and/or federal laws and regulations.
3. Running websites, blogs, or wikis that support commercial activities or running server systems under the CCSNH registered domain name, CCSNH.EDU or variation thereof, without authorization.
4. The use of the CCSNH name, seals, images and text are the property of CCSNH and shall not be used without the written permission of CCSNH.

Listservs, Bulletin & Discussion Boards

1. 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.

2. Posting chain letters of any type.
3. Forging header information on posts to listservs, bulletin or discussion boards.