Authorized Use of Campus Computing Resources
(Computer Resources Policy)

Applies To

Faculty, staff and student body

Licensing agreements for SUNY Cobleskill's computing environment authorize members of the faculty, staff and student body to use on-campus computing resources based on their academic and/or employment association with the college. Access to network resources, including but not limited to e-mail, data storage areas, research databases and other protected areas of the network, is provided as a convenience to facilitate access from residence halls, off-campus housing and other remote locations for campus-related activities only. All users who access campus resources have the responsibility to use them in accordance with the Campus Computer Resources Policy. Effective, efficient, ethical and legal use of any network account issued by SUNY Cobleskill is the responsibility of the person in whose name it is issued. Unauthorized use of computer services will be considered to be theft of services and will be dealt with according to the "appropriate campus disciplinary process" and/or Chapter 156 of the New York State Penal Law.

Responsible Use:

The privilege of using computing facilities at SUNY Cobleskill provides the campus community with access to tremendous educational, communicational and administrative resources. Network account holders are expected to use those resources in a responsible and efficient manner, consistent with the instructional, research, and administrative goals of the College. Use of computers and/or network facilities in ways that can impede computing access and activities for others is prohibited. Examples of such practices include, but are not limited to:

Wasteful Practices:

- Overuse of interactive network utilities during peak use times to engage in activities not related to course work or administrative functions of the college
- Tying up network printers with high volume print jobs
- Sending "Electronic Chain Mail" or unauthorized "Global" messages (e-mail sent to the entire campus)
- Interactive game playing on network resources during peak use times
- "Crashing" the system
- Failure to delete unnecessary files and e-mail messages to keep network accounts within allotted disk quotas.

Misuse of Resources: Destruction of, unauthorized removal of, or damage to equipment, software or data belonging to SUNY Cobleskill or other users. Tampering, modification or installing unauthorized programs to network software, hardware or wiring designed to disrupt or monitor electronic communications.

Recreational Use: Priority use of network resources, including but not limited to access to the Internet, e-mail, data storage areas and research databases, is given to students to complete class assignments and administrative offices to conduct college business.

Recreational use for non-competitive interactive game playing, casual "surfing on the Internet", use of chat lines, downloading of sound/video files and access to e-mail for personal use is allowable ONLY when it does not disrupt authorized campus activities

Unauthorized Servers:

The campus has the responsibility to protect the integrity of a very sophisticated and expensive computer infrastructure. The establishment of a background process that services incoming requests from anonymous users to download and/or share files/programs where that sharing is in violation of campus licensing agreements and/or copyright law is prohibited.

Examples of such practices include, but are not limited to:

- Running unauthorized FTP sites
- Running unauthorized DHCP servers
- Creating unauthorized web servers
- Establishing shares on personal computers to provide access to and/or unauthorized installation of programs not licensed to do so.

Private Commercial Purposes: Computer users may access campus resources for purposes related to academic or college business ONLY. The use of computing resources for commercial or personal financial gain without prior arrangements with the Director of Information Technology Services is prohibited.

Quotas: Although our servers are able to store massive amounts of information, there is a limit. The campus reserves the right to protect network resources by restricting storage space and placing quotas on all e-mail and data storage accounts to ensure fair access to network resources for college related activity and to prevent corruption of network system files.

Security

Maintaining security relative to access to centralized computing facilities is every user's responsibility. Users are expected to use ordinary precautions to protect their files from access and misuse by others.

- **Sharing of Network Accounts**: Unique usernames and passwords are assigned to individual network account holders to provide authorized access to computing resources. These accounts may **NOT** be shared with others.
- **Change Password Frequently:** Protection of passwords, data files and any activity initiated through network accounts is the responsibility of the account owner and is not under the control of the College. It is mandatory that account owners be careful to keep their accounts secure by changing their passwords frequently and keeping it secure.
- **Maintenance of System Integrity:** Users shall not intentionally develop, use programs or create unauthorized servers that infiltrate a computer system, promote unauthorized sharing of files and/or damage or alter the software components of a computing or network system.
- **Resource Accounting:** Accounting and security mechanisms installed on campus equipment have been established to protect access to system resources for all users. Users shall not develop programs or use procedures to alter or attempt to bypass the data-protection schemes that monitor the accounting and use of computer resources. Users may not employ means by which the facilities and systems are used anonymously or by means of an alias.
- **Report Abuses**: Users who are aware of unauthorized usage of system resources or suspect that someone else is using their account without permission should report such abuse to the Supervisor of Network Services.

Confidentiality

In general, information stored in network accounts is considered private, unless the account owner intentionally makes it available. The computing environment at SUNY Cobleskill is designed to protect user privacy, however, the College cannot and does not guarantee this result.

- **Respect for the Privacy of Others:** Users may not read, modify, copy, delete or otherwise access files or passwords from accounts belonging to others without the expressed consent or knowledge of the account owner.
- **Limitations:** There may be occasions when user data may become accessible to others. Examples of such access might include: access by system/help desk personnel while performing routine operations or troubleshooting, hardware/software failure or failure of the user to improperly log off network resources.
- **Disclosure:** SUNY Cobleskill strictly adheres to the guidelines for disclosure of confidential information as governed by the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) and New York State Open Records Statutes. Users found to be copying, modifying or otherwise accessing or distributing information for which they have not been granted permission will be liable to disciplinary action.

Copyright and Software Compliance

Because electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict compliance to copyright laws and software licensing agreements. SUNY Cobleskill strictly adheres to the intent, terms and conditions of Federal copyright law and software licensing agreements with it vendors.

- **Network Software Licensed for Campus Equipment Only:** Software available through the campus network and/or installed on campus owned equipment is licensed for use on campus computers ONLY. Any use of campus owned software on equipment not owned by the College without the expressed written permission from the publisher is in violation of the copyright law and is ILLEGAL.
- **Copying Networked Software Prohibited:** Users are NOT authorized to transfer, copy, modify or install copies of computer programs licensed to SUNY Cobleskill on personal equipment to avoid paying additional license fees. Any other use of campus owned software without the expressed written permission from the publisher is in violation of software compliance agreements and is ILLEGAL.

Digital Millennium Copyright Act

On October 28, 1998 President Clinton signed the Digital Millennium Copyright Act into law. Title II of the DMCA enables Online Service Providers (OSPs) to limit liability for monetary damages for copyright infringing activities of their users. Provisions within the legislation further protect educational institutions and limit liability for monetary damages caused by copyright infringing activities of their users. SUNY Cobleskill has taken the following actions to comply with Title II:

- Designated the Director of ITS, as our representative agent to receive notices from copyright owners about infringements.

- The Cobleskill home page has been updated to provide easier access to links referencing the Computer Resources Policy. Academic Ethics and Student Conduct Codes reflect relevant changes in new legislation regarding computer use/abuse.

- To make sure we are in compliance with copyright law, we are inventorying all “non-standard” software loaded on the campus network and checking to make sure all licensing and copyright compliance agreements are in order. Programs in question have been removed until evidence of proper licensing has been submitted to the ITS department for additional information)

  Web resources for the DMCA:

  http://www.arl.org/info/frn/copy/osp.html
  http://lcweb.loc.gov/copyright/onlinesp/

E-mail Policies

The ability to use electronic mail at SUNY Cobleskill is an important campus-wide resource. It is rapidly becoming an essential element in the college's day-to-day activities. Access to the computing resources in general, and electronic mail in particular is a privilege and must be treated as such by all users.

As with the use of other campus computing resources, abuse of these privileges can be a matter campus disciplinary procedures or outside legal action. Depending on the seriousness of an offense, violation of campus policy can result in penalties ranging from reprimand to loss of access and referral to college authorities or beyond for disciplinary action. In a case where unacceptable use severely impacts performance or security, in order to sustain reasonable performance and secure services for the rest of the campus users, the Supervisor of Network Services is authorized to immediately suspend individual access privileges until an investigation is completed.

Harassment: Sending threatening or unsolicited obnoxious or sexually explicit messages to others by e-mail is a form of harassment, as is continuing to mail someone after they have asked you to stop. You should never send anyone an e-mail message containing things you wouldn't say to him or her in person. Also, remember that what you consider humorous, others may consider offensive or even frightening. E-mail harassment violates ethical usage of your network account, and in some extreme cases may even provoke victims to press criminal charges. Harassing messages of a threatening nature will automatically be forwarded to University Police for further investigation.

Sending Global or "Mass" Messages: Although our e-mail client allows for the distribution of a single message to all computer users, posting of these "mass" or "global" e-mail messages, ties up valuable disk space, and greatly reduces system response time (sometimes to the point of crashing it). More importantly, many times these messages are perceived as harassment or electronic "junk mail" by most users and are deleted before they're read.

Posting of messages to the entire campus, (Global or "Mass" e-mail messages) without authorization constitutes irresponsible use of Campus Computing Resources and will result in the immediate suspension of your network account privileges.

Chain-mail: Chain-mail is another form of electronic junk mail. A chain-mail message is generally sent to several people and includes instructions that each person should forward the letter to several others. These messages waste system resources and often grow quite

large as senders append their own additions. The issue here has more to do with the potential for damage (wasted disk space, slowed network response time, etc.) than the fact that the message is being sent to a limited number of people.

While the intent of the originator is to send the message to just few people, it has the potential of becoming a global message if one of those recipients takes the message more seriously and decides to distribute it to everyone. Do not forward such messages. If you receive such a message at SUNY Cobleskill and would like to report it, forward the entire message to the Supervisor of Network Services.

Electronic Messages of a Threatening Nature:

- Don't panic. Try to remain calm so that you can get as much information as possible from the computer screen. This information may be vital in order to save lives or possibly apprehend the message sender.
- Treat any bomb threat as legitimate! It is not your job to determine whether or not the message is a joke.
- Copy the entire message EXACTLY as it appear on the screen. DO NOT hit any other keys. (If possible, print the screen.) Try to keep the message on screen.
- Call University Police at 5666 and relay the message EXACTLY as written. Try to hold the message on-screen until an officer arrives. Give him/her whatever information you have and be guided by his/her instructions.
- Understand that only the President or his designee can order a building evacuated for a bomb threat.

Virus Alerts: These types of messages represent one of the most common sources of globally distributed electronic chain mail. Unfortunately, the information is usually a hoax. Before you panic always consider the source. Do some research to verify whether or not the alert is legitimate. This is especially true of Internet sources since it is so easy for anyone to say anything, make up credentials, etc.

Ask yourself: Where does the information come from? Does this person have any credentials? Are they stating facts, opinions, or hearsay? If the information purports to be factual, what are the sources of the facts? Are they verifiable? There are other things you do when evaluating sources, but any one of these basic questions--which most careful readers review automatically--is sufficient to show your message as unreliable.

Use the Internet to search out information on the message's validity. Look for sites that have names and e-mail addresses of people to contact for more information. This makes it easy to contact them directly, or to verify their institutional affiliation. One reliable source of information is the U.S. Department of Energy Computer Incident Advisory Capability Site at:

http://www.ciac.org/ciac/ciac_virus_info.html

In short, there is a great deal of information indicating that many of these alerts are untrue. If you still have doubts begin by checking with the Computer Center staff, before you cry "Wolf!" and risk losing your access privileges. Additional information is available on the Knowledge Base.

Policy on Computer Viruses

It is the policy of SUNY Cobleskill to maintain the integrity of computing facilities against contamination from computer viruses by installing and regularly upgrading virus detection software on every campus owned computer. However, this cannot guarantee that equipment will not become contaminated in the future.

All who access campus computing facilities need to understand that all student labs are open to anyone with a valid account and as such access is "public" in nature.

Users who transfer data from diskettes used in campus computers to personal and/or business equipment are responsible to protect their equipment against the possible spread of viruses through the use of commercially available virus protection software.

In the event a major virus outbreak is identified/detected/suspected, the campus will be notified as quickly as possible.

- Warning notices will be posted in all Academic Computing labs outlining protection procedures and announcements will be placed in the Bulletin and What's Happening, and posted to Alerts Section of ITS's Web Page.
- Regular updates will be issued until campus equipment is totally disinfected.

Private, Commercial and Political Purposes

Computer users may access campus resources for purposes related to academic or college business ONLY. New York State Law prohibits use of campus computing resources for commercial or personal financial gain or to promote political agendas.

Fraud and Misrepresentation

Dishonest users sometimes attempt to forge mail messages to others to gain personal information, such as their account password or even credit card information. Do not ever divulge such personal data in a reply, even if the sender looks "official"; instead, forward the suspicious mail to the postmaster at the address where the message originated.

The College prefers not to act as a disciplinary agency or to engage in policing activities. However, in cases of unauthorized or irresponsible behavior, the College reserves the right to take remedial action, commencing with an investigation of the possible abuse, which may include temporary suspension of access privileges. Users, when requested, are expected to cooperate in such investigations. In cases of repeated abuse and severe violations to the Responsible Use Policy, students will be referred to the Student Judicial Board for further disciplinary action, which could result in the permanent loss of user privileges.

2007