Connecticut College

Appropriate Use Policy: Computer and Information Resources

Policy

Connecticut College information systems and resources (including computers, computer accounts, printers, networks, software, electronic mail, Web pages, WebCam, audio and video conferencing, and the telephone and voice mail systems) are for the use of Connecticut College students, faculty and staff. Users are encouraged to explore and utilize information systems and resources and to share their computer knowledge and expertise with other Connecticut College users. Resources may not be used for commercial purposes outside the scope of the College's mission.

The provision of information systems and resources at Connecticut College requires legal and ethical utilization by all users including faculty, students, staff, alumni and non-college account holders. The facilities at Connecticut College, including all central computing and telephone resources, the campus network, and all departmental resources are limited and should be used in a responsible manner. Many people depend on Connecticut College's computers and the voice and data network to complete essential parts of their work; therefore, users must not intentionally damage the system or misuse system resources so as to prevent others from doing their work.

The following list, though not covering every situation, specifies policies and regulations that govern usage of information systems and resources at Connecticut College and the networks to which Connecticut College is connected. All users are expected to abide by these regulations and policies and those that govern the use of the

campus computers, computer networks, labs, and the telephone and voice mail systems.

Use of Computing Resources

All users must comply with federal and state laws and all college regulations and policies related to any copying and use of computer software and electronic files. Connecticut College resources must not be used to violate the terms of license agreements and of copyright and trademark laws.

In addition, other activities that threaten the integrity of the system or harm individual users are not allowed.

Prohibited activities include, but are not limited to:

> Initiating or propagating electronic chain letters, unauthorized mass mailings (contact System Administrator for permissions/restrictions), or using e-mail or personal web pages for personal commercial purpose outside

the scope of the College's mission.

Falsifying your identity when sending a communication

Tampering with, abusing, or otherwise damaging computer or telephone hardware or software. This includes software or network tampering (hacking), such as attempting to crack or guess passwords, sending anonymous mail, or "bombing" a mailbox with multiple copies of a message.

Running or installing any program or sending any mass communication that overloads or substantially interferes with the proper operation of the computer system or network.

Overloading or substantially interfering with the proper operation of the College's network and computer data storage.

Using the College's computers or network or the telephone system to transmit fraudulent,

defamatory, harassing, obscene or threatening messages or any communications prohibited by law.

Improperly or inaccurately stating or implying the College's sponsorship or endorsement of any communications, including anything contained on a personal web page on the College's computers or network.

Engaging in activities that result in any direct cost to the College without prior authorization.

Users who publish web pages or similar information resources on the College computers or computer system shall take full responsibility for what they publish, shall abide by this policy and other College policies, shall comply with all applicable laws, and shall not publish commercial advertisements without prior written authorization. Links to commercial sites are permitted, but

advertisements are not. Users shall not accept any form of remuneration in return for placing anything on their web pages or similar facilities.

Security

Connecticut College computer and telephone systems are vital to the academic mission of the college. The information services staff members endeavor to maintain the integrity and proper functioning of the systems for the benefit of the College community.

A user must use only his/her own account. A user is responsible for all use made of his/her account, and may not authorize anyone else to use his/her account. The user must take all reasonable precautions, including password maintenance and file protection measures to prevent its unauthorized use.

The structure of accounts and passwords plays an important role in protecting the work and privacy of all users. You must log in only to your own account, except for extraordinary situations where

faculty or staff receive a user's permission to access their account temporarily or where use of a group account has been approved by the network administrator. In all other circumstances, you may not use another person's password or otherwise seek to gain access to another user's account.

Within means available, every member of the faculty, staff and student-body must take personal responsibility for maintaining the security of institutional records. Institutional records include all matters pertaining to personnel, payroll, registrar, admissions, financial aid, development, medical records, security reports, financial data and other information of privileged and private nature.

No one has the right or authority to extend his or her own established range of access to computer records. Users must not attempt to modify the system facilities or attempt to crash the system. They must not attempt to subvert the restrictions associated with their computer accounts. They must not tamper with any software

protection placed on any computer applications. They must not modify or delete data in a college data base without authority. This includes making changes to your own personal data in any college information system.

Users must not search for, access or copy directories, programs, files, disks or data belonging to others without specific authorization to do so. Programs and data residing in centralized college systems are not considered public domain and should not be used, in part or in whole, for any purpose other than that which is officially authorized.

Privacy

The College acknowledges its obligation – within the limitations of this policy and its ability – to respect the privacy of users' electronic files and communications on the College's information systems and resources. All system administrators shall respect the privacy of users and shall comply with the terms of this policy.

However, individual users of information systems and resources should be sensitive to the inherent limitations of shared network resources. No computer security system can absolutely prevent unauthorized persons from accessing stored information and the College cannot, and does not, guarantee the privacy or confidentiality of stored information or electronic communications.

The College has the right to monitor and access a user's communications, files, stored information and use of the system only under the following limited circumstances:

> When the user has consented, or has voluntarily made information or communications accessible to the public, as by posting them to a web page or listserv;
>
> When necessary to maintain college business functions and the employee is no longer with the college, is suspended, or is otherwise unavailable;

When required by law or by College policies or regulations, as reflected in the Information for Faculty, the Employee Handbook, or the Student Handbook;

When necessary to protect the integrity, security and proper functioning of the College's computers and networks or to protect the College from liability;

When necessary to enforce this policy or other College policies and regulations, as reflected in the Information for Faculty, the Employee Handbook, or the Student Handbook, including the College's sexual harassment policy and anti-discrimination policies, and to investigate when there is reasonable cause to believe that any of those policies or any state or federal laws has been or is being violated. A user's communications or files will be accessed for this purpose only with the prior approval of the Vice President for

Information Services or designee in consultation with the appropriate Senior Administrators.

When there is an existing College procedure that provides for an expedited review of alleged violations of law or College policies or regulations, that procedure will be used to determine whether it is appropriate to access a user's files or communications, unless exigent circumstances require immediate access.

If the College monitors or accesses a user's files or communications, it will respect information and communications that are privileged or otherwise protected from disclosure by law. Any monitoring or access to a user's files or communications will be no more extensive than necessary to accomplish the purpose for which it is authorized under this policy. Affected users will be notified of such monitoring or access provided that the notice is allowed by law and College policy and that it will

not compromise the College's investigation or an investigation of any law enforcement organization.

Other Applicable Rules, Laws

Users of the College's electronic resources, including E-mail communications, are subject to College policies and other statements of conduct as published in the Student Handbook, Faculty Handbook, and the Employee Handbook as well as all applicable federal and state laws. It should be understood that this Acceptable Use Policy does not supersede existing College regulations and policies – including the College's non-discrimination and sexual harassment policies – or the laws and regulations of the state of Connecticut and/or the United States of America.

Consequences

System administrators shall have the right to temporarily suspend any user's access to the system without notice where there is reasonable cause to believe such access poses a threat to the security

or proper functioning of the system or where it is necessary to comply with the law.

Violations of this policy or any other College rules on computer use will be considered grounds for removal of account and network privileges, and where appropriate, other disciplinary action. The College may revoke a user's account and network privileges for violations of law, of this policy or other College policies and regulations, only after notice and opportunity to be heard. Other possible disciplinary action will be determined through referral to the appropriate disciplinary authorities under existing College procedures.

Approved 2007

270 Mohegan Avenue
New London, CT 06320

1 (860) 447-1911

info@conncoll.edu
(mailto:info@conncoll.edu)

admission@conncoll.edu
(mailto:admission@conncoll.edu)

Web Privacy Policy (/web-privacy-policy/)