

## ISS Policies

### CLUnet Computer Use Policy

1999

Updated: August 17, 2007

Revised: 4/15/2009, 7/20/2009, and 7/7/2010

For a printer-friendly version of the Computer Use Policy,  
please [click here](#).

If you have questions about this policy, please contact the ISS Help Desk at (805) 493-3698 or send an [email](#).

- [Introduction](#)
- [Use of Equipment](#)
- [Use of Software](#)
- [Appropriate Access and Use](#)
- [Authorized Access](#)
- [Appropriate User Behavior \(Netiquette\)](#)
- [Plagiarism & Copyright](#)
- [The Rights and Responsibilities of Users and the University](#)
- [Reasonable Use of System Resources](#)

#### **INTRODUCTION**

CLUnet, the campus-wide information system at California Lutheran University, is designed to serve and foster the University mission of teaching, learning and public service, while supporting its administrative needs. This policy governs use of computing resources including computers and related equipment, as well as local area networks and connections to larger networks, specifically but not limited to the Internet. CLU honors and respects the privacy and academic freedom of its members, and strives to permit maximum freedom of use consistent with current University policy, and state and federal laws.

Access to CLUnet resources, whether local or remote, by CLU faculty, staff and students requires that individual users act responsibly and courteously and respect the rights of other users, the integrity of the information systems, and related resources. Complaints regarding misuse of CLUnet accessible resources will be directed to those responsible for taking appropriate disciplinary action. The Office of ISS will monitor network activity twenty-four hours per day, seven days per week. Some infractions, when accidental or through no obvious malicious intent, will be handled informally by the systems administrator. Other violations will be documented and referred through the Student Life Office, or the appropriate CLU administration or law enforcement authorities. Penalties range from reprimand, to loss of account, and to referral to University, state and/or federal authorities, for further action. Students and employees will lose account privileges while infractions are under investigation. Severity of punishment will be based on the infraction and/or history of infractions.

Unauthorized use includes illegal access to system files and files of other users, attempting to disrupt the integrity of the

system(s), and use of accounts belonging to other people. Misuse includes violation of federal or state law including the Digital Millennium Copyright Act and all other copyright laws, violation of University regulations, use of the system(s) for commercial purposes, displaying sexually graphic images or text, abusive language, harassing behavior, plagiarism, excessive use for non- official or frivolous purposes, and deliberately wasting or overloading computer resources.

## **USE OF EQUIPMENT**

CLU computing facilities and equipment are to be used only for University-related activities. All moves of or changes to equipment/software must be approved by ISS. Use for commercial purposes is neither authorized nor supported. Privately owned personal computers are the responsibility of the owner and not the University. Ownership and/or use of personal equipment, whether on or off campus, does not exempt the user from compliance with the CLUnet Computer Use Policy.

## **USE OF SOFTWARE**

The University has software licenses for the software that is available on CLUnet. Additions, removal, or transfer of such software without authorization is prohibited per U.S. Code, Title 17, Section 106. Users are required to use CLU-provided software as it was intended. Ownership or possession of illegal or damaging software, whether intentional or not, constitutes violation of the Computer Use Policy. Information Systems and Services will only provide support for University-approved software.

## **APPROPRIATE ACCESS AND USE**

Attempts to access unauthorized machines via the computer network, to decrypt encrypted materials, or to obtain privileges to which the user is not entitled (hacking) is prohibited per Public Law 98-473, Chapter XXI. Manipulation of files, access to unauthorized parts of CLUnet managed computers and network infrastructure, attempts to circumvent data protection schemes, to discover security loopholes, or possession of such software by users is prohibited.

## **AUTHORIZED ACCESS (Revised 7/20/09 & 7/7/10)**

Users are assigned one account for individual use. Sharing an individual computer account with other persons is prohibited. Passwords should be protected from discovery or use by others. If account holders knowingly or carelessly make their password available to others, they may still be held accountable for any actions that may arise from use of their account by another individual. Authorization for access will be canceled or modified when either a student terminates enrollment or fails to enroll for succeeding terms, or an employee separates from or changes job assignments at the University.

All accounts holders are expected to use strong passwords. Strong passwords have the following attributes:

- Minimum of 8 characters in length.
- Combination of both letters and numbers.
- Does not contain common dictionary words.
- May not be re-used (history tracking enabled).

Passwords must be re-set at least every 180 days for students and every 90 days for faculty, staff, and administrators or the account will be locked. Unlock your account or reset your password at the [MyCLU login page](#).

CLU through the Office of Information Systems and Services maintains control of domain name services. No University controlled IP address may be registered without University approval. ISS assigns all IP addresses, and any unassigned IP will be disconnected.

## **APPROPRIATE USER BEHAVIOR (NETIQUETTE)**

Users of CLUnet resources, including but not limited to electronic mail, bulletin boards, or discussion groups, are prohibited from sending or displaying messages or images that are libelous, patently offensive, or sexually explicit, or that intimidate, threaten, demean, or are defamatory or (4/15/09) harass individuals or groups, or that would otherwise bring discredit to the University. Refer to the Campus Policy on Harassment in the Student, Faculty, and Staff Handbooks.

## **PLAGIARISM & COPYRIGHT**

Plagiarism of electronic works (e.g., text, graphics, programs) is prohibited. Copying of works without attributing credit to the author is cheating and constitutes academic dishonesty. Refer to the Academic Honesty Policy in the Student, Faculty, and Staff Handbooks.

The University also enforces the Digital Millennium Copyright Act. Reports of copyright infringement should be sent to the Associate Provost of Information Services.

## **THE RIGHTS AND RESPONSIBILITIES OF USERS AND THE UNIVERSITY (Revised August 19, 2007)**

A person's directory, files, and E-mail are to be considered private property, and therefore, confidential. Any attempt to access, monitor, read, copy, change, or delete files or mail without explicit permission of the account holder is prohibited.

Although users have individual passwords to access voice mail, E-mail, computer programs and the like, the University does not guarantee complete confidentiality in those transmissions. The University will honor your privacy, but reserves the right to monitor communications and/or usage when there is just cause, e.g., to remove or compress inappropriate or large files, to investigate user directories and files which may cause or be affected by a system problem, may be suspected of unauthorized use or misuse, or may be corrupted or damaged. User files may be subject to search under court order if such files are suspected of containing information that could be used as evidence in a court of law.

The University will back up user data stored on the personal and shared directories on CLUnet central servers, and bears no responsibility for loss of user data due to system failure, user error or any other cause.

Users are responsible for backing up personal files stored on laptop and desktop computers. Exchange server email is backed up. Messages deleted in Outlook or Entourage remain on the central server for 30 days.

## **REASONABLE USE OF SYSTEM RESOURCES**

Users should not consume unreasonable amounts of limited resources. Space and time on CLUnet systems will be fairly distributed among users, and may fall under system-imposed quotas. Each dorm resident may connect only one personal computer using Mac OS 10.x, Windows 2000/ME/XP workstation to CLUnet. Sub-networks in residence halls are not permitted. ISS has responsibility for establishing all physical connections for CLUnet connected pc's and will maintain an inventory of MAC (media access control) addresses. Unregistered MAC addresses will be disconnected from CLUnet. Users may request additional storage space based on legitimate University-related use, subject to verification from ISS. Printing is limited to one original copy. Inactivity at a computer for 15 minutes will result in the user being logged off. Dial-in users are asked to restrict access to CLUnet for a maximum of one hour per day.



