KECK GRADUATE INSTITUTE
A Member of The Claremont Colleges

Campus Computing and Network Resources Policy

KGI Policy
KGI is committed to responsible, considerate and ethical use of computing and networking resources. KGI and The Claremont Colleges make available computing and network facilities (CNF) resources for use by students, faculty, and staff, to carry out the educational mission and legitimate business of the Colleges. We expect and require that all KGI users will demonstrate responsible, considerate, and ethical behavior in using these resources.

KGI follows The Claremont Colleges Policy Regarding Appropriate Use of Campus Computing and Network Resources. The Claremont Colleges Policy below applies to all institutions comprising The Claremont Colleges, including The Claremont Colleges Services.

Inappropriate use is subject to disciplinary action. KGI or any Information Technology organization of one of The Claremont Colleges may immediately suspend service to an individual or computer found to be significantly degrading the usability of the network or other computer systems. Inappropriate use will be referred to the appropriate College authority to take action, which may result in dismissal from school and/or termination of employment.

Claremont Colleges Policy
General Provisions
An overall guiding mission of The Claremont Colleges is education in an environment where the free exchange of ideas is encouraged and protected. The Claremont Colleges make available computing and network facilities (CNF) resources for use by the Colleges' students, faculty and staff. These services are provided for educational purposes and to carry out the legitimate business of the Colleges.

The Colleges and members of the college communities are expected to observe Federal, State, and local laws that govern computer and telecommunications use, as well as the Colleges' regulations and policies. You must not use campus computing or networking resources or personal computing resources accessed through campus network facilities to collect, store, or distribute information or materials, or to participate in activities that are in violation of federal, state, or local laws or other college policies or guidelines.

These include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment. Computing and network facilities resources users are required to use these resources within the Colleges' standards of conduct. Individuals with expert knowledge of information systems or who make extensive use of these facilities, or with a position of trust regarding these facilities will be held accountable to a higher standard. Responsible, considerate, and ethical behavior expected by the Colleges extends to use of computing and network facilities resources, and networks throughout the world to which electronic access has been provided. These CNF resources include but are not limited to:

- Computers and associated peripheral devices
- Campus video cable
- Classroom presentation systems

- Voice messaging equipment
- Data networking equipment systems, including remote and wireless access
- Computer software
- Electronically stored institutional data and messages
- All other similar resources owned, controlled, and/or operated by the Colleges, and
- Services to maintain these resources

Ownership of CNF Resources
The Colleges retain absolute ownership rights of the CNF resources. Such resources are not owned by a department or by any individual. CNF resources leased, licensed, or purchased under research contracts or grants, are administered under the terms of this Policy for as long as they remain within the lawful possession or control of the Colleges. CNF resources provided to on-campus residences are also owned, operated, and provided by the Colleges.

Privacy and Security
FILE CONFIDENTIALITY
Your documents, files, and electronic mail stored on a College-owned networked computer or server are normally accessible only by you. However, any file or document placed on a College owned
computer or network is subject to access pursuant to this Policy, and thus, should not be regarded as private or confidential. The system managers at both CINE (Claremont Intercollegiate Network Effort) and within the individual campus IT organizations have the ability to monitor traffic and directly view any file as it moves across the network, and they must occasionally do so to manage campus network resources. In short, files may be monitored without notice in the ordinary course of business to ensure the smooth operation of the network.

All staff members working in information technology have clear guidelines that prohibit violations of privacy and confidentiality and, in the normal course of their work, they do not view the contents of user files or e-mail. However, you should be aware that authorized College personnel will take appropriate steps to investigate when there is a suspicion of inappropriate use of campus computing or networking resources. This may include monitoring network traffic, its contents, and examining files on any computer system connected to the network.
You should also know that all files on shared (i.e., networked) systems, including e-mail servers, are backed up periodically on schedules determined by each College. Backup tapes are preserved for lengths of time also determined by individual College operating procedures. These tapes can be used to restore files that you have deleted accidentally.
This means that the files on the tapes are also available to someone else with reason and authority to retrieve them.

NETWORK MONITORING
Troubleshooting on the campus network, as well as planning for enhancements, requires the collection of detailed data on network traffic. CINE regularly runs monitoring software that records and reports on the data that is transported across the campus networks. The reports include the origin and destination addresses, and other characteristics of files, including the URLs of the World Wide Web sites that are contacted. This data is accessed and used only by authorized IT staff members responsible for network performance, operations, and planning.
You should also be aware that many Web host machines on the Internet collect and log

information about you and your identity when you visit their sites. This information may include, but is not limited to, information about the computer you are using, its address, and your e-mail address.

Many educational and business activities at the Colleges require network access to resources on the Internet. To ensure adequate bandwidth to these sites for the Colleges' primary educational and business purposes, CINE and campus IT staff may restrict the amount of traffic to particular sites and the amount of traffic of specific types.
From time to time these network monitoring activities may allow systems managers to identify individuals whose activities downgrade the performance of the campus network or a segment of the network, or which appear to violate the general guidelines for appropriate use of campus computing and network resources. In such instances, a CINE staff member or a member of your own College's IT staff may ask you to cease these activities. If you continue such activities, or if they include illegal activities, appropriate College authorities may be notified. In extreme cases, network privileges may be revoked on an interim basis pending resolution of the issue. The individual campuses determine specific corrective or disciplinary actions.

PASSWORDS AND CODES
Individuals entrusted with or that inadvertently discover logins and passwords are expected to guard them responsibly. These passwords are not to be shared with others. The same policy applies to door codes for restricted-access rooms/areas. Those who need logins or door codes can make a formal request to the administrator of those codes/passwords. Passwords may be used for the purpose of security, but the use of the password does not affect The Claremont Colleges ownership of electronic information.

ACCESS TO RESOURCES
Access to CNF resources is a privilege, which is allowed only to the Colleges' authorized personnel and students. All users must understand and abide by the responsibilities that come with the privilege of use. Such responsibilities include, but are not limited to, the following:

- You must understand and comply with all applicable federal, state, and local laws.
- You must not intentionally seek information about, browse, copy, or modify non-public files belonging to other people, whether at a Claremont College or elsewhere. You must not attempt to "sniff" or eavesdrop on data on the network that are not intended for you.
- You are authorized to use only computer resources and information to which you have legitimately been granted access. Sharing your passwords with others is expressly forbidden. Any attempt to gain unauthorized access to any computer system, resource, or information is expressly forbidden. If you encounter or observe a gap in system or network security, immediately report the gap to the manager of that system.
- Each College's Policy on Harassment applies as equally to electronic displays and communications as to the more traditional (e.g., oral and written) means of display and communication.
- Messages, sentiments, and declarations sent as electronic mail or postings must meet the same standards for distribution or display as physical (paper) documents would on college property.
- Unsolicited mailings and unauthorized mass mailings from campus networks or computing resources (i.e., "spam") are prohibited. Each campus may have specific policies regarding the use of existing group mailing lists (e.g., all-students or all-faculty). Contact your campus IT organization for details regarding these policies.

• Spoofing, or attempts to spoof or falsify e-mail, network, or other information used to identify the source, destination, or other information about a communication, data, or information is prohibited.
• You must not degrade computing or network performance in any way that could prevent others from meeting their educational or College business goals. You must not prevent others from using shared resources by running unattended processes, by playing games or by “locking” systems without permission from the appropriate system manager.
• You must conform to laws and Colleges policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks.
• When the content and distribution of an electronic communication would exceed fair use as defined by the federal Copyright Act of 1976, users of campus computing or networking resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.
• You must not use campus computing or networking resources or personal computing resources accessed through campus network facilities to collect, store, or distribute information or materials, or to participate in activities that are in violation of federal, state, or local laws.
• You must not use campus computing or networking resources or personal computing resources accessed through campus network facilities to collect, store, or distribute information or materials in violation of other Colleges policies or guidelines. These include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment.
• You must not create or willfully disseminate computer viruses, worms, or other software intended to degrade system or network security. You must take reasonable steps to prevent your system from being used as a vehicle for such actions. This includes installing system and software patches as well as anti-virus signatures files.
• Use of CNF resources for advertising, selling, and soliciting for commercial purposes or for personal gain is prohibited without the prior written consent of the Colleges. Faculty, students, or staff who have questions about the legitimacy of a particular use should discuss it with the appropriate members of the IT staff on their home campus.
• The disclosure of individually identifiable non-directory information to non-university personnel is protected by the Family Educational Rights and Privacy Act of 1974(FERPA). The disclosure of financial or personnel records that are owned by the Colleges without permission or to unauthorized persons is not permitted and may be prosecuted under California Penal Code 502.
• Willful or unauthorized misuse or disclosure of information owned by the Colleges will also constitute just cause for disciplinary action, including dismissal from school and/or termination of employment regardless of whether criminal or civil penalties are imposed. It is also expected that any user will report suspected abuses of CNF resources. Failure to do so may subject the individual to loss of CNF access and/or the disciplinary action referred to above.