CLAREMONT McKENNA COLLEGE

Policy Library

Volume X:	Information Technology Services
Chapter Network:	Use of Internet Services and Network Resources
Approved by:	Information Technology Committee (ITC)
History:	Issued: AY 1998-1999 Reformatted/Revised by ACC: 12/14/2009
Related Polices:	Claremont Colleges Policy Regarding Appropriate Use of Campus Computing and Network Resources, Student Computing Laboratory Usage Policy, Student Residential Network Use
Additional References:	N/A
Responsible Official:	Office of Information Technology Services

I.   POLICY STATEMENT

-       The computer resources of any of the Claremont Colleges may *not* be used for commercial purposes. Faculty or staff who have questions about the legitimacy of a particular use should discuss this with the appropriate individuals on their campus. Campus computer resources -- including individual desktop machines -- may *not* be used to collect, store, or distribute information in violation of federal, state, or local laws. Since the laws about such matters as copyright, pornography, etc., are evolving, it is not possible to give definitive guidelines in all cases at this time. Caution and common sense will usually be adequate guides but, if you are in doubt, you should seek advice before proceeding.

II.   ENTITIES COVERED BY THIS POLICY

-       The Claremont Colleges' connection to the Internet is managed centrally by Harvey Mudd College through CINE (the Claremont Intercollegiate Network Effort). CINE serves as a conduit for all traffic into and out of the Claremont Colleges, including e-mail, Web, FTP, etc. This traffic is routed to servers at each campus, and is then distributed to users by your own college's information technology office. Use of these services is governed by "Claremont Colleges Appropriate Use of Campus Computing and Network Resources" approved by the Council of Presidents in 1995; copies are available on your college's Web site. All faculty, staff, and students are urged to familiarize themselves with this document.

III. CONTACTS

Direct any questions about this policy to your department's supervisor. Questions about specific issues may be addressed to:

Subject	Contact	Telephone[1]
Use of Internet Services and Network Resources	Chief Technology Officer	71553

IV.   DEFINITIONS

Confidentiality of Files on the Network

- Your documents, files, and electronic mail messages stored on a networked computer or server are normally accessible only to you; they are protected from unauthorized "prying eyes." However, systems managers at CINE 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. Managers at each college (including, at some campuses, students working under the supervision of professional staff) have similar capabilities to monitor files as they traverse their local campus networks and to view files stored on shared systems. This is necessary for the smooth operation of the network. All staff members working in information technology offices 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. However, you should be aware that your files may be viewed by a person with such privileges if there is a need to do so.

V.   Monitoring Internet Use
- Troubleshooting on the network, as well as planning for necessary enhancements, requires the collection of detailed data on network traffic. At the request each college, CINE regularly runs monitoring software that records certain information about all network packets transmitted through its facilities. The software produces reports that include the names, origins (by IP address), destinations, and other characteristics of all files it detects, including the URLs (addresses) of the World Wide Web sites that are contacted. These reports are accessed and used only by authorized staff members with responsibilities for overseeing the network, and are important for network operations and planning. Similar network diagnostic procedures may also be conducted on local networks by your campus' IT staff. You should also be aware that many Web host machines on the Internet log similar information about your identity when you visit their sites. This information may include your e-mail address.

- From time to time, monitoring activities on the Claremont network may lead systems managers to identify individuals whose activities downgrade the performance of the network or appear to violate the General Guidelines for Appropriate Use of Campus Computing and Network Resources. In such instances, you may be asked by a member of the CINE staff or your own college's information technology staff to cease this activity. If the activity continues, or if illegal activities are detected, appropriate college authorities may

---

[1] Numbers refer to on-campus extensions. When calling from an off-campus line, please dial (909) 62+extention for numbers beginning with a "1" and please dial (909) 60+ extension for numbers beginning with a "7."

be notified. In extreme cases, network privileges may be revoked on an interim basis pending resolution of the issue. Specific corrective or disciplinary actions are determined by the individual campuses.