CLAREMONT McKENNA COLLEGE

Policy Library

Policy Regarding Appropriate Use of CMC's Computing and Network Resources

Volume:	Information Technology
Chapter:	Policy Regarding Appropriate Use of CMC Computing and Network Facilities Resources
Approved by:	Administrative Computing Committee
History:	Issued: September 13, 2011
Related Polices:	The Claremont Colleges Policy Regarding the Appropriate Use of Campus Computing and Network Resources; Anti-Virus Policy; Configuration of Out-of-Office Message; E-Mail Distribution Lists; E-Mail Signature Block Standard; Submitting Mass E-Mails to Claremont McKenna College
Responsible Official:	Chief Technology Officer

I. POLICY STATEMENT

Users of computer and network facilities (CNF) resources provided by The Claremont Colleges and Claremont McKenna College have a responsibility to properly use and protect those information resources and to respect the rights of others. The Claremont Colleges Policy Regarding the Appropriate Use of Campus Computing and Network Resources (the "Consortium's Appropriate Use Policy") provides general standards related to the appropriate use of CNF resources across the Consortium as a whole. This Policy Regarding the Appropriate Use of CMC Computing and Network Resources (the "CMC Appropriate Use Policy") provides additional standards related to the use of CMC's CNF resources. The CMC Appropriate Use Policy shall supersede the Consortium's Appropriate Use Policy to the extent that there is any conflict between the two policies.

II. ENTITIES COVERED BY THIS POLICY

All individuals utilizing Claremont McKenna College's CNF resources.

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]
Policy Clarification	Chief Technology Officer	71553

IV. POLICY DISCUSSION

CMC's information technology infrastructure is designed and provided for the purposes of supporting the basic mission of Claremont McKenna College in teaching, learning, and research.

Because these resources leverage each individual's ability to access and copy information from remote sources, users must be mindful of the rights of others to their privacy, intellectual property and other rights. The Consortium's Appropriate Use Policy and the CMC Appropriate Use Policy together describe what is considered appropriate usage of CMC's CNF resources. With the privilege to use CMC's CNF resources come specific responsibilities as outlined in these Policies. In addition, although reasonable and limited personal use of the College's CNF resources is recognized, personal use of the College's CNF resources shall not be permitted when it disrupts or conflicts with the primary educational and business purposes for which they are provided. Finally, as noted above, the CMC Appropriate Use Policy shall supersede the Consortium's Appropriate Use Policy to the extent that there is any conflict between the two policies.

A. *Ownership:* CMC retains ownership and property rights to its CNF resources.

B. *Access to Resources:* Access to CMC's CNF resources is a privilege provided to authorized users of the College's CNF resources, including students at The Claremont Colleges, CMC faculty and staff, and other authorized users. With this privilege, all users of CMC's CNF resources shall understand and abide by the responsibilities that come with the privilege of use. These responsibilities are generally set forth in the Consortium's Appropriate Use Policy, and are incorporated herein by reference; provided, however, that the following additional specific standards shall apply to the use of CMC's CNF Resources:

1. The College reserves the right to inspect and monitor data and communications at any time, for any reason it determines in its sole discretion. This includes monitoring network usage, including contents, and examining files on any system that is or has been connected to the network. Accordingly, no individual should have any expectation of privacy for messages or other data recorded in the CMC's CNF Resources.

[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."

2. No use of CMC's CNF Resources should ever conflict with the primary business and educational purpose for which they have been provided or with applicable laws and regulations.

3. The use of CMC's CNF Resources to create, transmit, or store material that is fraudulent, harassing, obscene (e.g., pornographic), threatening, or other messages or material that are a violation of applicable law or College policy, such as under circumstances that might contribute to the creation of a hostile academic or work environment, is prohibited. Such prohibition includes the viewing or downloading of pornographic material.

4. This Policy shall not be interpreted to prohibit the appropriate use of CMC's CNF resources in a manner that would unreasonably restrict a faculty member or student's teaching, learning, and research, or such individual's academic freedom.

5. CMC's Office of Information Technology Services (ITS) reserves the right to immediately suspend service to an individual or computer determined by ITS to be degrading the usability of CMC or CUC CNF Resources.

6. A user of CNF Resources who is found to have violated this Policy will be subject to disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, pursuant to the relevant procedures given the status of the user. If system administrators have information of misuse of CNF Resources, and if that information indicates the computing activities or the computer files of an individual, they should pursue one or more of the following steps, as appropriate to protect other users and the College's CNF Resources:

    a. Provide notification of the investigation to the College's Chief Technology Officer or designate as well to the Dean of the Faculty if the user is a faculty member, the Dean of Students if the user is a student, and Human Resources if the user is a staff member.

    b. Temporarily suspend or restrict the user's computing privileges during the investigation. Faculty members may appeal such suspension or restriction through the Dean of the Faculty, students may appeal through the Dean of Students, and staff members may appeal through Human Resources.

    c. With authorization from the Chief Technology Officer or designate, inspect the user's files, diskettes, tapes, and/or other computer-accessible storage media on College owned and operated equipment.

    d. Refer the matter for possible disciplinary action to the appropriate College unit, i.e., the Dean of the Faculty for faculty members, the Dean of Students for students, and Human Resources for staff.