Computer Policies

The Claremont Colleges
General Guidelines for Appropriate Use
of Campus Computing and Network Resources

The Claremont Colleges make available computing and network resources for use by the Colleges' students, faculty and staff. These services are to be used only for educational purposes and to carry out the legitimate business of the Colleges.

Those who avail themselves of the computing and network resources are required to use them in a manner consistent with the Colleges' standard of conduct. Individuals who possess expert knowledge of information systems or who make heavy use of these facilities, or who are in a position of trust regarding these facilities will be held to particularly high standards of conduct.

The framework of responsible, considerate, and ethical behavior expected by the Colleges extends to cover the use of campus facilities and network resources, and networks throughout the world to which electronic access has been provided by the Colleges.

Files may be monitored in the ordinary course of business. In addition, when there is reason to suspect inappropriate use of campus computing or networking resources, authorized College personnel will take steps to investigate. This may include monitoring traffic on the network, including contents, and examining files on any system which has connected to the network.

The following list does not cover every situation which pertains to proper or improper use of the resources, but it does suggest some of the responsibilities which you accept if you choose to use the Colleges' computing resources or the network access which the Colleges provide.

- You must not intentionally seek information about, browse, copy, or modify files or passwords belonging to other people, whether at the Claremont Colleges or elsewhere.

- You are authorized to use only computer resources and information to which you have specifically been granted access. If you encounter or observe a gap in system or network security, you should report the gap to the manager of that system immediately.

- If it is unclear whether you have permission to copy, compile or manipulate software or data, assume that you may not do so.

- The Colleges' policies on harassment apply equally to electronic displays and communications as they do to more traditional means of display and communication. You must not display, or transmit images, sounds or messages that could create an atmosphere of discomfort or harassment for others.

- Messages, sentiments, and declarations sent as electronic mail or postings must meet the same standards for distribution or display as tangible documents.

- You must not degrade computing or network performance in any way that will prevent others from meeting their educational or college business goals.

- You must not create or willfully disseminate computer viruses. You should be sensitive to the ease of spreading viruses and should take steps to insure your files are virus-free.

The above statements are not intended to serve as an exhaustive list. Members of the college community are also expected to observe Federal, State and local laws which govern computer and telecommunications use, as well as the Colleges' own regulations and policies.

Approved by the Council of the Claremont Colleges 6/7/95

Computer Policies

CGU Administrative Computing Policies

Access

Claremont Graduate University is the owner of all administrative computing systems and the data contained within. This includes the personal computers located in employee offices as well as the network servers such as the administrative VAX, email post office, or Windows NT servers. An employee's access to these systems and data is defined and limited by the department granting access. The requirements of the employee's job will determine how much access that person is given. By accepting access to the administrative computer systems of Claremont Graduate University, employees acknowledge acceptance of the responsibilities defined in both the General Guidelines for Appropriate Use of Campus Computing and Network Resources and the CGU Administrative Computing Policies.

Monitoring

As owner of all administrative computing systems and data contained within, Claremont Graduate University reserves the right to monitor the use of all computing systems to maintain security.

Confidentiality

All data residing on administrative computers is for official business of Claremont Graduate University, and as such, should only be released during the course of official business. Records of faculty, students, staff, or donors of Claremont Graduate University are confidential. Employees may not disclose any of this information to any party except as part of the official business of the University.

Accounts and Passwords

Access to data on administrative computer systems is limited through the use of user accounts and passwords. When a user is given an account, it is their responsibility to keep their password secret. Users should observe the following "established password practices:"

NEVER give your username and password to another person.
Do not leave your terminal or PC logged on and unattended.
NEVER write down your username and password.
Change passwords frequently.
Make passwords unique and difficult to guess.

Software

All software running on administrative computing systems must be licensed by Claremont Graduate University. CGU employees should not install any software on any administrative computers without prior approval of Administrative Computing. In addition, employees may not commit unauthorized copying of software or data. (Certain licenses of certain software packages may allow the user to have a copy at work and at home. Check with Administrative Computing to find out which software this applies to.)

Backup

Although Claremont Graduate University is the owner of all data residing on administrative computing systems, CGU employees share some of the responsibility for backing up that data. Backup of data residing on servers is the responsibility of Administrative Computing and is accomplished by Administrative Computing personnel. This includes the administrative VAX, the Millennium server, the Microsoft Mail Post office, the PowerFaids server and the SPARC servers. Backup of data residing on individual PCs in CGU offices is the responsibility of the individual employee who uses that PC.

Claremont Graduate University Academic Computing Policies

Responsibility for Files: While Academic Computing at CGU will make every effort to provide reliable places to store data being used for academic work, it takes no responsibility for maintaining or recovering any files of any student, faculty, or staff member stored on any computer on the CGU campus. It is the responsibility of each individual user to make backup copies of their own files. We urge everyone to do so. Academic Computing is ready to assist in showing clients how to back up their data and to help in cases of data loss, but the ultimate responsibility of data lies with the owner of that data.

Addition of Software to Computers: Clients should not install any software on any computers on the CGU network without prior approval of Academic Computing. They should not modify software on the computers in any way. Doing either of these things may result in the loss of all computing privileges. A specific need to run a piece of software not currently on CGU computers should be addressed to Academic Computing: we will do what we can to accommodate the need.

Abuse of Network Privileges: Use of the CGU network or the Internet to do any kind of damage to any computer on these networks or to threaten or harass any user on any computer or for non-academic purposes will result in the temporary or permanent loss of all computing privileges at CGU.

Games: No playing of computer games is allowed in any of the labs. This includes Internet games such as MUDD and MUSH games. Playing of a game designed to produce network or individual computer problems will result in immediate loss of computer privileges at CGU.

Accounts: No computing accounts should be used by anyone other than the owner. Provision of an account name and password or other access to an account issued by CGU Academic Computing to someone other than the owner is grounds for loss of all computing privileges.

CGU'S WORLD-WIDE WEB RELATED POLICIES

COPYRIGHT AND DISCLAIMER

Claremont Graduate University's Web site provides a wide range of information about the University. While every effort is made to maintain complete, up-to-date, and accurate information, the University reserves the right to change its programs, costs, and policies as necessary.

The views and opinions expressed on personal pages are strictly those of the authors. Claremont Graduate University does not edit or pre-approve personal pages and accepts no responsibility for the contents therein.

CGU'S WORLDWIDE WEB POLICIES

What is the WWW Site Statement of Purpose of the CGU Web Site?

The purpose of the Web site is to foster the achievement of CGU's mission through enhancing (a) teaching, (b) research, and (c) the administrative functions needed to support these objectives.

It should only be used for purposes directly related to the achievement of the institution's objectives.

What is the Content of WWW?

WWW is an electronic "publication" of CGU and as such is subject to the same content requirements of other publications. Only materials that will help achieve the purpose of the site are allowed to be published.

The CGU Web site consists of four distinct, but related, parts:

Institutional pages are edited and maintained by individual departments. They include but are not limited to the home page, student affairs pages, policy pages, and pages which provide links to the departments and schools.

Departmental and school pages are those pages that are linked from the institutional pages but are maintained by designated departmental coordinators. The Web Communications Manager supports these coordinators.

Personal pages may be posted on the CGU Web server by faculty with the understanding that those pages provide information relevant to the individual's role at the University. Personal Web pages are subject to the same policies applied to other Web pages and publications. Note

especially that pages on University servers may not be used to promote personal business or to provide personal financial gain.

Personal pages shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University.

An appropriate disclaimer is:

> The opinions or statements expressed herein should not be taken as a position or endorsement of Claremont Graduate University.

All sites under University jurisdiction (i.e., on Claremont Graduate University servers) must display information on the ownership of the sites, including a contact name with email address, and the date of the last update. If the site consists of more than one page, the ownership information should appear on all pages of the site.

Who is Responsible for the Web Site?

The responsibility for recommending policy and determining access to and use of the Web site is vested in the Web Committee which reports to the IT Steering Committee.

COPYRIGHT INFRINGEMENT COMPLAINTS

In accord with the Digital Millennium Copyright Act (DMCA), allegations of copyright infringement on Claremont Graduate University's web site locations should be reported to our designated agent:

Director of Information Technology
Claremont Graduate University
150 East Tenth Street
Claremont, CA 91711-6160

Phone: (909) 621-8077
Fax: (909) 607-9821