CLAREMONT McKENNA COLLEGE

Policy Library

Volume X:	Information Technology Services
Chapter Network:	Student Residential Network Use
Approved by:	Administrative Computing Committee (ACC)
History:	Issued:09/01/01 Revised: 12/20/06; 02/28/07 Reformatted/Revised: 12/14/2009
Related Polices:	Student Computing Laboratory Usage Policy, Use of Internet Services and Network Resources
Additional References:	N/A
Responsible Official:	Office of Information Technology Services

I. POLICY STATEMENT

- To establish the responsibilities of individuals or groups who attach computer systems or other devices to the Claremont McKenna College student residential computer network.

II. ENTITIES COVERED BY THIS POLICY

- This policy covers all persons attaching computer systems to Claremont McKenna College student residential network.

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]
Student Residential Network Use	Chief Technology Officer	71553

IV. DEFINITIONS

- The student residential network is a shared, finite resource installed by Claremont McKenna College to promote scholarship and learning for all students. Accidental or intentional disruption of the residential network will

[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."

deprive others of access to important Internet and Intranet resources. Persons attaching computers to the Claremont McKenna College student residential network must comply with the *Use of Internet Services and Network Resources*, the *Claremont McKenna College Computing Usage Policy, Claremont McKenna College's Basic Rule of Conduct*, and other College policies. Violation or disregard of these policies may result in disconnection from the network and, if serious enough to warrant disciplinary action shall be referred to the Dean of Students Office. Illegal activities may be reported to the appropriate civil authorities for prosecution.

V. DETAILS

- Computers attached to student residential network have to adhere to the following rules:

1. Identity: all personally owned devices connected to the CMC network will be required to register with ITS in order to provide the Network Administrator with the information necessary to contact individual users in the event that his/her computer is causing a network problem. Registration will be handled automatically at the time a computer is connected to the campus network. All network services and resources will be unavailable until the device is registered. The registration process will be required at the start of each academic year and whenever a device is moved to a new location on the network.

2. Hosting any server/service is strictly prohibited without prior approval by ITS.

3. Responsibility for Content: The content of any files made available to others over the network is the sole responsibility of the person with ownership of, and/or administrative authority over, the computer providing the files. It is this person's responsibility to be aware of all applicable Federal laws, State laws and College policies. This person will be liable for any violations of Federal laws, State laws, or College policies. Such violations, including copyright violations, may be subject to criminal prosecution.

4. Commercial Use: The use of student residential network facilities for commercial use is strictly prohibited.

5. Computer names must be non-profane and non-offensive.

6. Network-Intensive Applications: Any person operating a network-intensive application or a defective computer, either of which overloads the networks, will be notified and steps will be taken to protect the overall Claremont McKenna College network. This may include throttling, traffic shaping, or disconnecting the offending computer system from the network until the problem is resolved. If the condition is an imminent hazard to the College network or disrupts the activities of others, then the offending computer system or the subnet to which it is attached may be

disconnected without prior notice. This latter course of action may affect many other persons connected to the network.

7. Responsibility for Security: Any person attaching a computer to the student residential network is responsible for the security of the computer system and for any intentional or unintentional activities from or to that network connection. Anti-virus software must be installed in compliance with the “Anti-Virus Policy.” www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/gemavtp.pdf