CLAREMONT McKENNA COLLEGE

Policy Library

Volume X:	Information Technology Services
Chapter Other:	Student Access to Administrative Information Systems
Approved by:	Senior Staff ITC
History:	Issued: 01/09/1999 Updated: 10/14/1999 Reformatted by ACC: 12/14/2009
Related Polices:	Change Management Policy, CMC's Response to Student Violations of the Digital Millennium Copyright Act, Complying with the Digital Millennium Copyright Act, Employee Termination Information Access and Resource Disposition
Additional References:	N/A
Responsible Official:	Office of Information Technology Services

I. POLICY STATEMENT

- To prohibit student access to administrative computing systems, workstations and networks.

II. ENTITIES COVERED BY THIS POLICY

- All students**,** faculty, and staff at Claremont McKenna College.

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 Access to Administrative Information Systems	Chief Technology Officer	71553

IV. DEFINITIONS

[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."

Administrative computing systems store most of Claremont McKenna College's confidential**/**sensitive data. This includes personnel, financial, alumni, donor, student, and parent data. It is the responsibility of the College to maintain and ensure the security of these data. Only authorized employees of the College may have access to these data. The phrase "authorized employees" does not include student employees. Although we place great trust in student employees and believe that they will not abuse any privileges that we might grant them, they do represent a security risk and therefore must not be allowed any type of access to these sensitive data. Students will not be given access to employee workstations. These workstations are on the administrative subnet and allow students access to the flow of sensitive data and administrative computing systems. Also, these workstations maintain sensitive data that must be safeguarded.

V. DETAILS

The following procedures will be used to ensure that students do not come in contact with sensitive administrative data:

1. Students **will not** be given an account on the main administrative central computer systems.
2. Employees of the college **will not** allow students access to the central computer systems via the employee's account.
3. Students **will not** be given access to employee workstations that are either on the administrative subnet or store sensitive data.
4. Any workstations set up for student use will not be connected to the administrative network.
5. Any employee that knowingly allows a student access to these systems will be **subject to disciplinary action up to and including termination of employment**.

VI EXCEPTION

If it is absolutely necessary for a student employee to have access to administrative workstations, the administrative network and/or central computers, then a formal request, in writing, must be submitted to the CTO of Information Technology Services by the head of the requesting office. If it is determined by the CTO of Information Technology Services that it is necessary for that student employee to gain access to administrative resources, then only minimal access will be granted. The head of the requesting office and the CTO of Information Technology Services will meet and establish the minimal access needed for the student employee to accomplish their jobs. Final approval will be given by the President.