

FITC Access Agreement Form

The CATS Faculty Instructional Technology Center is provided as a place for faculty to receive assistance in developing digitized materials to enhance teaching and learning. Student web developers (the "WebDev" group) and staff assist faculty, and expensive digital equipment is available in this central facility. We foster a collaborative atmosphere of sharing ideas, sharing equipment, sharing space. Therefore, we ask faculty using this room to complete the following agreement to minimize problems when no technical staff are on duty to assist. This form must be completed before Omnilock and alarm codes are issued, and the agreement will be renewed (and new codes given) on July 1 of the new fiscal year..

1. I will not give my Omnilock or alarm code to anyone.
2. I will not allow others to enter the Center if they do not have their own access
3. I will not install or delete software from any of the machines without prior approval.
4. I will not plug or unplug any equipment in or out of the computers and peripherals without prior approval.
5. I will not leave files on the workstations. I understand that any files left on the Macintoshes and Pentium are not backed up and may be deleted at any time.
6. I will not store more than 50MB total on the "www.ic" and WebCT web servers.
7. I know how to log on to ic server to upload my files. (Using WS-FTP, FETCH, or AppleShare.).
8. I know that workstations are reserved each quarter. I will sign up for a workstation when I use it. If someone has reserved the workstation but has not arrived within 10 minutes of the reserved start time, they will relinquish their ho has not reserved their workstation must relinquish it to whomever may have reserved it within 10 minutes of the reserved start time.
9. I know that machines are secured with a fiber loop which will set off the security alarm if stretched. To avoid setting off the alarm, I won't move the machines in the FITC.
10. I acknowledge that I will be financially responsible for any charges resulting from any alarms I set off.
11. Any materials that I need to leave in the room will be left on a shelf labeled with my course name and number, not at the computer workstations.
12. I understand that printing is available at CATS computer labs. Printing costs 15 cents per page. You will need to pay for prints via a Slug Copy Cardin all IC computer labs (FITC does not have Slug Card capabilities, printing will be recharged with consulting hours.)
13. I will only use the room during the designated "open hours" and "assisted hours" as set each quarter. I will not be in the room during hours when it is designated to be not accessible. I will use the online workstation scheduling form to make specialize equipment reservations.
14. I understand that I may receive up to 4 hours free assistance (by appointment) per quarter. Recharges apply for more than 4 hours assistance per quarter.
14. I understand I must comply with campus computing guidelines, including copyright restrictions/laws and Americans with Disabilities Act guidelines.
15. I verify that I know how to:

use the Omnilock to open the door	use the alarm panel to secure and unsecure the FITC
turn the workstations on	shut down workstations (and will, before leaving the FITC)
turn the peripherals on and off	to reset power strips, should the power go off
take auto feeder on and off the slide scanner	use Zip drives, CD-ROM and floppy drives
16. If I am the last one to leave the FITC, I will close all windows and turn on the alarm
17. I will not leave food and drink next to the workstations. When I leave the FITC, I will take all food/drink garbage with me. I won't leave food/drink in the waste can to prevent insects/smell.
18. I will comply with the Policies for Use of UCSC Computing Facilities. These policies specifically exclude using any computing staff, facilities, or other resources for commercial or political purposes, or using these resources for personal gain.

Name _____ Department and Title

Signature _____ Date

Policies for Use of UCSC Computing Facilities

It is the policy of the University of California to provide computer resources to students, faculty and staff to be used in ways that are consistent with the University's mission -- instruction, research, and public service -- and in activities that support that mission, such as administration. These resources include computers, terminals, networks, modems, and printers.

It is the policy of the University to provide its users with access to local, national, and international sources of information in an atmosphere that encourages sharing of information, access to a rich collection of services, and open and free discussion.

The University expects that its user community will respect the public trust through which these resources have been provided. The work and efforts of the user community should not be subject to unauthorized disclosure, tampering, destruction, theft, harassment, nor should there be a denial of access to resources.

All users of campus computing resources share in the responsibility to protect the rights of the entire community. All users must guard against abuses of the University's information resources and systems.

The University has determined that the following list, while not exhaustive, characterizes unacceptable behavior which may be subject to disciplinary action:

1. Use of any University facilities in a manner that violates copyrights, patent protections, or license agreements;
2. Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;
3. Any violation of state law as described in the Penal Code, as an example, a copy of Section 502 of the California Penal Code is available separate from this policy statement;
4. Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;
5. Any action that disrupts the availability of a system for others, such as running programs that utilize all system resources and prevent others from making productive use of the system;
6. Any use of University computing facilities for personal gain (including advertising) or political purposes without the prior approval of the University;
7. Any use of University computing facilities to harass others;
8. Attempts to alter, damage, delete, destroy or otherwise abuse any computer or network resource.

In addition, the user should be aware of the following policies and expectations:

The University grants permission to members of its community to use computation resources by issuing individual computer accounts. As a condition of receiving such an account, the user must exercise diligence to keep his or her password as a secret and not disclose it to any other person. Users of shared computers or networks which connect to the campus network should not share or transfer their

The University expects that all those who choose to use our off-campus network connections will understand and honor the policies of those regional and national network organizations to which the University is a party. The use policies for these networks are available separately from this policy statement.

Campus units that administer computers may also establish guidelines for the appropriate use of their equipment in addition to these campus wide policies. Those guidelines must be consistent with campus wide policies.

When a non-University-owned computer is used on campus, the user must follow all of these campus wide policies. In addition, if the computer is attached to the campus network¹ it must be registered with the owner's name and contact information, machine manufacturer and model number, location of machine, and the network address of the machine. This registration can be done through divisional computer/network managers or through CATS.

¹ This includes computers with one or more unique network addresses as well as computers that obtain network addresses on a dynamic basis.