

CCSF COMPUTER USAGE POLICY

Copies of this CCSF Computer Usage Policy can be found in the college catalogue and the employee's handbook. Each user who uses the CCSF computing facilities and resources is bound by this policy. This policy is displayed to users via Message of The Day (MOTD) in the first two weeks of each semester at their logon to the CCSF HPUX computer system.

Violation of these policies will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the College, and legal action. Violations of some of the policies below may constitute a criminal offense.

Rights and Responsibilities

CCSF is pleased to make computer accounts and resources available for student use in the pursuit of their instructional goals, and to faculty and staff to support the institution's instructional goals. In so far as the computing resources are under the user's control, the user is fully responsible for their proper and legal use.

The Computer Usage Policy applies to all members of the College community using our computer resources. This includes administrators, faculty, staff and students. This includes use of computer equipment at any CCSF facility including in the various computer labs, classrooms, offices, libraries and the use of the CCSF servers from any location.

Computer accounts and computer access are privileges, and require the individual user to act responsibly. By using the CCSF accounts, users have agreed to respect the rights of other users and accounts, to use the account only for school-related purposes, and to safeguard the integrity of the system and its related physical resources. Users have further agreed to observe all relevant laws, regulations, policies and contractual obligations of the College.

Other organizations operating computing and network facilities that are reachable via the City College network may have their own policies governing the use of those resources. When accessing remote resources from City College facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations. It is the user's responsibility to be informed of the policies of other outside organizations to which they establish a computer link.

Confidentiality

All user files, including e-mail files, are not to be relied upon as confidential. CCSF explicitly does not guarantee or warrant the confidentiality of these files. It is the practice of Information Technology Services (ITS) to respect the confidential nature of user files, but the ITS Department reserves the right to view or alter user files when it is necessary. Any ITS employee must have their manager's permission prior to investigating a user file.

User files may also be subject to search under court order if such files are suspected of containing information that could be used as evidence in a Court of law. Student files as kept on ITS facilities are

considered educational records as covered by the Family Educational Rights and Privacy Act of 1974 (Title 20, Section 1232(g) of the United States Code, also referred to as the Buckley Amendment).

In addition, a system administrator may access user files as required to protect the integrity of the computer system. For example, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

Existing Legal Context

All existing federal and state laws and College regulations apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

Misuse of computing, networking or information resources may result in the loss of computing and/or network privileges without notice. This includes both those that ITS administers, and those that may exist in other departments associated with City College of San Francisco and connected to its network. Deliberate violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary sanctions including, but not limited to, loss of computer use privileges, dismissal from the college, and/or appropriate legal action.

Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable College or campus policies, procedures, or collective bargaining agreements. Complaints alleging misuse of the College's computing resources will be directed to those responsible for taking appropriate disciplinary action as specified under Enforcement below. Illegal reproduction of software protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment (See CCSF Policy Manual 8.10).

Copyright

All users must follow all relevant copyright laws. US Copyright law governs reproduction and distribution of software and other material, including text, fonts, graphics, sound, video and others. The End User License Agreement (EULA) for a product specifies the conditions under which a user may copy or install the product. The EULA purchased by a department also controls the number of simultaneous users of the product. Please review the EULA for complete information on your rights as an end user of these products.

Nondiscrimination

Computer users need to follow the same non-discrimination policy including those governing "sexual harassment" & "hostile education environment".

All computer users must follow the non-discrimination guidelines as stated in the CCSF "Equal Opportunity Statement" listed in the catalog: <http://www.ccsf.org/Policy/nondiscrim.html>

Any user who files a complaint or otherwise protests against discrimination has the right to be free from any retaliatory action because of the complaint or protest. The CCSF administrator who receives a complaint of discrimination should inform the complainant of this right and that the complainant may file an *additional complaint* if he or she experiences *retaliatory conduct*.

Examples of misuse include, but are not limited to, the following activities:

Breaking into another person's account

1. Using a computer account that you are not authorized to use by the ITS Department. Knowingly or carelessly allowing someone else to use your account.
2. Obtaining a password for a computer account that is not your own account.
3. Using the Campus Network to gain unauthorized access to any computer systems.
4. Attempting to circumvent data protection schemes or uncover security loopholes. This includes creating running and/or distributing programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
5. Masking the identity of an account or machine. This includes, but is not limited to, sending e-mail anonymously.

Harassment

6. Using e-mail to harass others.
7. Posting on Internet services information that may be slanderous or defamatory in nature. This includes, but is not limited to, posting of said type of material on Usenet News.
8. Displaying sexually explicit, graphically disturbing, or sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.

Commercial use

9. Using your account for any activity that is commercial in nature. Commercial activities include, but are not limited to, consulting, typing services, and developing software for sale.

Copyright

10. Violating terms of applicable software licensing agreements or copyright laws.

Changing files

11. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner. Files owned by individual users are to be considered private property, whether or not they are accessible by other users.
12. Modifying of another user's files, which is illegal under California Computer Crime Laws.

System misuse

13. Sending mass e-mail to a large number of people on the system. It is acceptable, however, to use organization or department mailing lists, listserves, to send e-mail to groups of people on the system.
14. Knowingly or carelessly performing an act that will interfere with the normal operation of computer systems, including running, or installing, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes programs known as computer viruses and worms.

15. Deliberately wasting/overloading system resources, such as:
- Printing resources - This includes, but is not limited to, printing multiple copies of a document or printing out large documents that may be available on-line, or that might impact significantly on other users printing resources.
 - System file space - Storing or transferring of large files or using a large amount of file space in the temporary file system area which degrades overall system performance or preclude other users right of access to disk storage also constitute misuse of resources. The ITS staff may remove or compress disk files that are consuming large amounts of disk space, with or without prior notification.

Additional System Information

- Batch jobs or background tasks should be consistent with individual academic goals or institutional academic goals. Jobs that do not appear to coincide with the academic goals of the institution may be "killed" without warning.
- Any files stored in the temporary file systems are not backed up and are subject to deletion at any time. Users' file names and directory names starting with a period or another punctuation or special character will be deleted immediately.

Enforcement

After the appropriate investigation and/or hearing procedures have been followed, the penalties below may be imposed under one or more of the following: City College regulations, California law, the laws of the United States.

- Infractions of the CCSF Computer Policy may result in the temporary or permanent loss or modification of computer account and resource access privileges, and may be subject to further disciplinary action.
- Offenses which may be in violation of local, state or federal laws will result in the immediate loss of all computer account and resource privileges, and will be reported to the appropriate College or institution involved and law enforcement authorities.

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be *confidentially reported* to the appropriate supervisors or instructor and/or department chair.

Related documents

- Disclaimer, URL: <http://www.ccsf.org/Policy/disclaim.html>
- Equal Opportunity Statement, URL: <http://www.ccsf.org/Policy/nondiscrim.html>
- Web Site Standards & Practices, URL: <http://www.ccsf.org/Policy/standards.html>
- Web Page Development Guide, URL: <http://www.ccsf.org/Policy/guidelines.html>
- Web Design Guidelines, URL: <http://www.ccsf.org/Policy/webguidelines.html>

This document is subject to revision. The Information Technology Policies Committee approves changes to the guidelines, as needed.