APPENDIX A

CCSF Computer Usage Policy

This policy is displayed to users upon their initial logon to the CCSF computer systems and each user must agree to it in order to continue to use the CCSF computing facilities.

Rights and Responsibilities.

CCSF is pleased to make computer accounts and resources available for student use in the pursuit of their 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.

Computer accounts and computer access are a privilege 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 their 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.

Confidentiality

Misuse of computing, networking, or information resources may result in the loss or termination of computing services without notice. Additionally, misuse can be prosecuted under applicable statutes. Users will be held accountable for their conduct under any applicable district or campus policies and procedures. Deliberate violation 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.

All user files, and especially 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 Information Technology Services office of CCSF (ITS) reserves the right to view or other 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. In addition, a system administrator may access user files as required to protect the integrity of the computer system. Student files as kept on ITS facilities are considered educational records as covered by the Family Education Rights and Privacy Act of 1974 (Title 20, Section 1232g) of the United States Code, also referred to as the Buckley Amendment. For example, system administrators may access or examine files or accounts that are suspected of unauthorized use of 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, network, or information resources may result in the loss of computing and/or network privileges, 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.

Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable College or campus policy, procedure, or collective bargaining agreement. Complaints alleging misuse of ITS 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

U.S. Copyright Law bans illegal reproduction and distribution of software. Computer software may be copied only for back-up purposes, if permitted by the copyright owner. Distribution of the copies can be provided only to registered users. The number of simultaneous users corresponds to the number of original licensees purchases by the department.

Other organizations operating computing and network facilities that are reachable via 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 whom they establish a computer link.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of CCSF computing systems which discriminates against any person on the basis of race, color, national origin, sex, or disability.

Discriminatory conduct includes, but is not limited to, written or graphic conduct that satisfies both of the following conditions: (1) harasses, denigrates, or shows hostility or aversion toward an individual or group based on the person’s gender, race, color, national origin, or disability, and (2) has the purpose or effect of creating a hostile, intimidating, or offensive educational environment. “Harassing conduct” and hostile educational environment are defined below.

“Harassing conduct” includes, but is not limited to, the following: epithets, slurs, negative stereotyping, or threatening, intimidating, or hostile acts, that relate to race, color, national origin, gender, or disability. This includes acts that purport to be “jokes” or “pranks” but that are hostile or demeaning.

A “hostile educational environment” is established when harassing conduct is sufficiently severe, pervasive, or persistent so as to interfere with or limit the ability of an individual to participate in or benefit from the CCSF computing systems.

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

Using a computer account that you are not authorized to use by the ITS Department.

Obtaining a password for a computer account that is not your own account.
Using the Campus Network to gain unauthorized access to any computer system.

Knowingly or carelessly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.

Knowingly or carelessly running or installing on any computer system or network, 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.

Attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

Violating terms of applicable software licensing agreements or copyright laws.

Deliberately wasting/overloading computing 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.

Using electronic mail to harass others.

Moving large files across networks during peak usage periods or prime hours such that it degrades resource performance. Prime hours will be considered to be Monday through Friday from 10:00 a.m. to 5:00 p.m.

Storing large files on the systems which could compromise system integrity or preclude other users' right of access to disk storage. The ITS staff may remove or compress disk files that are consuming large amounts of disk space, with or without prior notification.

Masking the identity of an account or machine. This includes, but is not limited to, sending mail anonymously.

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.

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. 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.

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.

Logging in on more than one session at a time.

Modifying another user’s files, an illegal act under California Computer Crime Laws.

Additional System Information

Batch jobs or background tasks should be consistent with individual academic goals or institutional academic goals. Jobs which 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 any time. User file names and directory names starting with a period will be deleted immediately. User files/file trees which contain information more than four days old or the directories themselves which exceed four days of age will be deleted.

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 such as sharing accounts or passwords, harassment, or repeated minor infractions as described in, but not limited to, the above policies may result in the temporary or permanent loss or modification of computer account and resource access privileges, and notification of a student’s academic advisor and/or the department chairperson in the case of staff or faculty.

More serious infractions, such as unauthorized use, harassment, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of the College policies, or repeated violations as described in the above paragraph may result in the temporary or permanent loss of CCSF computer accounts and resources. In all cases, the offender’s associated school or department and/or the Dean of Students will be notified of the infraction to pursue further disciplinary action.

Offenses which are 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 supervisor or instructor and/or department chair.

Violations
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 above policies may constitute a criminal offense.

Complaint Procedure:
Any user who believes he or she has been subject to discrimination on the basis of race, color, national origin, gender, or disability may inform the system administrator or the City College of San Francisco. Upon receiving any such complaint, CCSF shall process the complaint through the Dean of Students Office in accordance with the CCSF “Discrimination and Grievance” Procedures.

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 CCGS 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.
This document is subject to revision. The Computer Policy Committee will approve addition of more or deletion of guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval, and other items related to administering the system.