

## **General Policies on University Computer Resources**

### ***1. General Statement***

1.1 The goal of Information Technology Services and campus departments administering university computer resources is to promote innovation and educational excellence at California State University, Fresno. To achieve this, the computing network must provide quality and cost-effective information and communication resources to the members of the university community.

1.2 The university endorses the following statement of Software and Intellectual Rights that was developed through EDUCOM, a non-profit consortium of colleges and universities committed to the use and management of information technology in higher education.

1.2.1 “Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.”

1.2.2 “Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secrets copyright violations, may be grounds for sanctions against members of the academic community.”

1.3 The above statement provides a guide for the ethical use of computer facilities whether one is using a microcomputer, minicomputer, mainframe computer or supercomputer, or computer network, and whether the computer files, programs, or data are stored on floppy disk, hard disk, magnetic tape, or other storage media. Computer facilities and files owned by others should be used or accessed only with the owner’s permission.

1.4 The university’s computing facilities are provided for the use of students, faculty, administration, and staff and to some extent to members of the wider community, in support of the programs of the university. All students, faculty, administrators, and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical and lawful manner.

1.5 The possession of a computer account carries with it certain conditions and responsibilities which this policy statement endeavors to explain. Misuse of accounts or violation of the delineated conditions may result in the termination of the accounts, or, in cases of more serious infractions, the submission of the case to an appropriate disciplinary authority for further investigation. In such cases, because different laws, policies, and procedures govern appropriate actions involving students, faculty, administrators, or staff, any appropriate actions

must follow the appropriate procedures (for example, the various collective bargaining agreements governs appropriate actions involving faculty and staff members and specifies specific procedures).

1.6 Computer facilities and accounts are owned by the university and/or its various schools, departments, auxiliary organizations, and programs, and are only to be used for university-related activities. All access to central computer systems, including the issuing of passwords, must be approved through ITS or the designated administrator for the central system. Accounts for other resources, such as department or school-owned resources, are given out by those entities.

1.7 An account assigned to an individual, by ITS or a department, must not be used by others. The individual is responsible for the proper use of the account, including proper password protection.

1.8 The university's intent is to consider programs and files as private and confidential unless they have explicitly been made available to other authorized individuals, but it is impossible to insure such materials against all security violations. As a practical matter, the appropriate systems administrator may access others' files when necessary for the maintenance of central computer systems. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if violations are discovered, they will be handled through normal university procedures.

1.9 Electronic communications cannot be considered either private or secure. E-mail messages can be saved indefinitely on the receiving computer. Copies can easily be made and forwarded to others either electronically or on paper. In addition, messages sent to nonexisting or incorrect usernames are delivered to a person designated as Postmaster for either the remote or local site. In sending e-mail, it is the user and not the university, who assumes responsibility for its contents. E-mail communications may be subject to discovery in civil litigation or in criminal investigations. In most instances, there is no reason for e-mail to be retrieved by anyone other than the intended addressee, but in limited and appropriate circumstances (e.g., in the course of an official investigation of wrongdoing), e-mail messages may become subject to internal monitoring by an authorized individual.

1.10 Electronic communications facilities (such as e-mail) are for university related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored. No e-mail should be created or sent, nor webpages created, that may constitute intimidating, hostile, or offensive material on the basis of gender, race, color, religion, national origin, sexual orientation or disability. The university's policies on sexual or other forms of harassment apply fully to the e-mail systems, including those involved with electronic mail and the Internet.

1.11 California State University, Fresno supports academic freedom and the free exchange of ideas, in conformity with federal and state law. The content of home pages on the Internet is solely the responsibility of the authors and does not necessarily reflect policies or opinion of the

university. It is unlawful to affix the university seal to any material without prior approval from the university.

1.12 Unmannerly or unprofessional conduct using the computer account is inappropriate; for example, mailing obscene or abusive messages is not considered acceptable behavior. Also disallowed are random mailings (spamming). Internet and other network users must also abide by the respective guidelines for those services.

1.13 The university computer facilities (laboratories, offices, the Library, etc.) do not provide a private environment for accessing e-mail or Internet resources. Therefore, users are advised to be aware of their responsibilities for appropriate behavior in public places. Some materials, which may be appropriate for scholarly inquiry in various disciplines, reasonably may be seen to have a strong possibility of creating a hostile environment for other students, faculty, staff, and visitors.

1.14 No one should deliberately attempt to degrade the performance or capability of a computer system or to deprive authorized personnel of resources or access to any university computer system. Loopholes in the computer system, knowledge, or special passwords shall not be used to damage a system or file, or to change or remove information in a system or file without authorization.

1.15 Attempting to attain unauthorized access to another's directories or files or in any way attempting to "break" system security is deemed unacceptable behavior, even if it is for purposes of "browsing" only and not for acquiring data. If a user is able to circumvent the system security, it should be considered an obligation to inform the department administering the system or other appropriate authority of this possible breach.

1.16 Computer software protected by copyright is not to be copied from, into, or by using campus computing facilities, except as permitted by law or by a license agreement with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies. The number of copies and distribution of the copies may not be done in such a way that the number of simultaneous users exceeds the number of original copies authorized.

1.17 University computer resources should never be used for purposes intended to incite or commit a crime; for example, it is illegal to post a credit card number, a telephone credit card number, or a computer password. Criminal and illegal use may include obscenity, child pornography, threats, harassment, theft, and unauthorized access\*. In addition, the networks cannot be used for personal profit; for example, do not use a discussion list to advertise items for sale or to solicit business.

---

\* Reference California Penal Code 502

**2.     *Violations***

2.1    Violations of this policy will be handled through normal university procedures.