



June 26, 1997
**EXECUTIVE
MEMORANDUM
97-18**

From: Manuel A. Esteban, President
Subject: Executive Memorandum 97-18, **Policy on Use of Computing and Communications Technology**

On the recommendation of the Academic Senate and Provost Scott McNall, I approve EM 97-18, Policy on Use of Computing and Communications Technology, for immediate implementation.

**POLICY ON USE OF
COMPUTING AND COMMUNICATIONS TECHNOLOGY
CALIFORNIA STATE UNIVERSITY, CHICO**

DEFINITIONS

Computing and communications -- These terms include voice, data, and video networks, switches, routers, and storage devices and any and all forms of computer-related equipment, tools, and intellectual property, including computer/communications systems, personal computers, and all forms of software, firmware, operating software, and application software which is owned by the University or is in the University's possession, custody, or control.

Electronic communications -- This term refers to the use of computers and communications facilities in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools.

POLICY

Scope

This policy includes all systems/resources for both local departmental and central universitywide facilities and applies only to institutional data and/or equipment. This policy does not apply to computing equipment that is the property of faculty, staff, and students except that the use of personal equipment linked to university facilities (e.g., a personally owned microcomputer linked to the campus network) will be subject to applicable provisions. In all cases, applicable statutes and regulations that guarantee either protection or accessibility of institutional records will take precedence over this policy.

Purpose

The purpose for computing and communications systems, services, and facilities at California State University, Chico is to support the educational and service mission of the University. This policy sets forth users' rights and responsibilities and is designed to address related access, use, and privacy issues in a way that meets the University's legal responsibilities, assures the maintenance of the campus network systems, and treats the campus community with respect. This policy assumes as a condition of use the exercise of common sense, common courtesy, and a respect for the rights and property of the University and other users.

Access

Access to the university's computing and communications facilities and resources is a privilege granted for the purpose of educational use and legitimate university-related business to university faculty, staff, currently registered students, and to individuals or organizations outside the University who are actively involved in research, development, or other projects sponsored by a department, college, or the institution. Retired faculty and staff will be granted continued access to computing and communications

facilities, but such access under certain circumstances may require modifications due to limited resources. Faculty and staff whose employment status has been terminated will not retain any form of access.

Legal Basis

Use of the university's computing and communications facilities and resources is governed by all applicable CSU system and university policies and procedures, as well as by all applicable federal, state, and local laws and statutes. Users are subject to the California State University 4CNet Acceptable Use Policy. 4CNet provides access to the network infrastructure that interconnects CSU campuses and other sites to information and communication resources worldwide.

Material accessible to the CSU, Chico community through networks and material disseminated from CSU, Chico should not be restricted on the basis of its content (with the exception of content otherwise prohibited by law, e.g., pornography, defamation, etc.) nor because of the origin, background, or views of those contributing to its creation. University administrators, faculty, and staff should challenge any attempts to censor electronic information resources.

Privacy and Ownership (Disclaimers)

The University supports each individual's right to private communication and will take reasonable steps to ensure security of the network. However, messages on university computing resources are potentially accessible to others through normal system administration activities, in response to subpoenas or other court orders, and to the public through public records laws. Hence, the University cannot guarantee absolute privacy of electronic communication.

The University supports each individual's right to privacy of personal files. However, in the normal course of system administration, the administrator may have to examine user files to gather information to diagnose and correct problems. Additionally, with reasonable cause for suspicion and appropriate administrative authority, files may be examined by system personnel to determine if a user is acting in violation of the policies set forth in this document, other university policies, or state or federal statutes. The University cannot guarantee that, in all instances, copies of critical data will be retained on university systems. It is ultimately the responsibility of computer users to obtain secure, backup copies of essential files for disaster recovery.

The University will normally treat all e-mail messages, personal files, and personal data as private and confidential and will normally examine or disclose the contents only when authorized by the affected computer user(s). Requests for access to private messages/data for any other purpose than technical problem resolution will be approved by the senior Academic Affairs Officer or his/her designee, except as necessary to protect the integrity, security, and effective operation of the university's computing and communications facilities or as required by local, state, or federal law.

To protect the integrity, security, and effective operations of the university's computing and communications facilities and the users thereof against unauthorized or improper use of these facilities, the University reserves the right, without notice, to limit or restrict any individual's use of any computing and communications facility or resource and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine security, integrity, or the effective operation of the university's computing and communications facilities. The University disclaims responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of computing and communications facilities.

Caution: Having open access to computing and communications facilities implies some risk. The University cherishes the diversity of values and perspectives endemic in an academic institution and is respectful of freedom of expression. Therefore, it does not condone censorship nor does it endorse the inspection of files other than on an exceptional basis. As a result, the University cannot protect individuals against the existence or receipt of material that may be offensive to them. However, users are subject to the appropriate university policies regarding harassment (EM 99-20). Reasonable expectations of privacy are diminished once electronic communications are sent to other users or posted on public systems. Like a written communication, an e-mail message received by an individual will be considered the prerogative of the recipient to dispose of (copy, delete, save, send to others, etc.) as he/she desires. An electronic message should be accorded care and courtesy similar to that accorded a written communication.

University-purchased, -owned, or -maintained software for individual workstations and site licenses, data, and custom applications programs are the exclusive property of the University and shall be used by faculty, staff, and registered students only in the conduct of university business.

User Responsibilities and Acceptable Use

Each faculty, staff, and student user of CSU, Chico's computer communications systems is responsible for the material that he or she chooses to send or display using the campus computing/communications resources. All personal data processed is considered sensitive and/or confidential. Anyone utilizing/accessing university computer systems, related data files, and information shares the responsibility for the security, integrity, and confidentiality of information.

Acceptable use of computing and communications facilities and resources at CSU, Chico includes Respect for the legal protections provided by copyright and licenses to programs and data as well as university contractual agreements.

Respect for the rights of others by complying with all university policies regarding intellectual property (e.g., EM 83-08) and the university code of ethics.

Using accurate identification in all electronic communications to avoid deliberately misrepresenting any user's identity.

Respect for the privacy of student records by complying with all university policies regarding student records (e.g., EM 01-01).

The University has subscribed to the statement on software and intellectual rights distributed by EDUCAUSE, the non-profit consortium of colleges and universities committed to the use and management of information technology in higher education, and ITAA, the Information Technology Association of America, a computer software and services industry association:

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to work 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.

"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 secret and copyright violations, may be grounds for sanctions against members of the academic community."

The following guidelines further pertain to the appropriate use of campus computing and network services.

Threats, Harassment*. Users may not use campus computing or network services to threaten, harass, defame, or otherwise interfere with the legal rights of others.

(*Harassment is defined as the creation of an intimidating, hostile, or offensive working or educational environment.)

Public Areas. Users should take care not to display on screens in shared facilities images, sounds, or messages which could create an atmosphere of discomfort or harassment to others. Users should make arrangements for a private work area if an assignment requires them to access such materials.

Respect for Privacy. Users must respect the privacy of other users. Examples of lack of respect for the privacy of others include reading their mail, accessing their files, or using their computer account or electronic mail address (except as may be required in the case of university employees for the purpose of facilitating official university business).

Sharing of Account. Users may not share their password with others or let others use their account (except as may be required in the case of university employees for the purpose of facilitating official university business).

Academic Honesty. Users must respect the intellectual property of others and adhere to university standards of academic honesty. Examples of academic dishonesty include accessing or using the files of others without their permission, altering or destroying their files or messages, violating standard citation requirements for information accessible electronically, or using copyrighted software in violation of the copyright agreement.

Illegal/Incompatible Uses. Users may not use computing and network services for uses that are inconsistent, incompatible, or in conflict with state or federal law, CSU policy, or university policy.

System Disruption. Users must not intentionally disrupt the campus computing system or obstruct the work of other users, such as by interfering with the accounts of others, introducing or spreading viruses or

other destructive programs on computers or the network, sending chain letters or blanket e-mail messages, or knowingly consuming inordinately large amounts of system resources. Operational Procedures. Users must respect the university's operational procedures for computing and network services. Users are responsible for knowing and abiding by posted computer lab and network procedures. Generally, operational procedures prohibit printing multiple copies of documents on networked printers and playing games in labs when others are waiting for systems. Finally, as instructional use is paramount, users must leave a lab when it is needed by a class that has reserved the room in advance.

Colleges, departments, and other areas within the University are responsible for seeing that their communities are aware of this policy and its acceptable use provisions.

Sanctions and Disciplinary Actions

Any unauthorized use of or damage to or disruption of any state computing and/or networking system is in violation of the California Penal Code and is subject to prosecution. University faculty, staff, and students who violate any of the above policy also may be subject to disciplinary action following established university channels for disciplinary matters. Individuals who violate U.S. copyright law and software licensing agreements also may be subject to criminal or civil action by the copyright or license owners.

Actions that are illegal or against university policy will be referred to the appropriate officials regardless of whether or not a computer was involved in their commission.

The University may track user activities and access any files or information in the course of performing normal system and network maintenance or while investigating violations of policy or statute. Anyone using CSU, Chico's resources expressly consents to such tracking and is advised if such tracking reveals possible evidence of criminal activity the University will provide the evidence to law enforcement officials. A system administrator may find it necessary to suspend or restrict a user's computing or communications privileges during investigation of a problem. A user may appeal such suspension or restriction and petition for reinstatement of computing and communications privileges through the University's administrative process, through the grievance procedures outlined in the University's collective bargaining agreements, or through the student grievance procedures as appropriate.

Violators are subject to any and all of the following:

Loss of computing and networking access

University disciplinary actions

Civil proceedings

Criminal prosecution

Offenders may be prosecuted under laws including (but not limited to)

The Computer Fraud and Abuse Act of 1986

The Computer Virus Eradication Act of 1989

Interstate Transportation of Stolen Property Act

The California Criminal Code

The Electronic Communications Privacy Act

Reporting Policy Violations

If a person believes that a violation of this policy has occurred, he/she should contact the system or network administrator responsible for the system or network involved, or the department manager if data confidentiality is involved, who will report the incident to the college/unit policy officer in accordance with local procedural guidelines, should they exist.

There may be situations when the following additional offices should be contacted:

University Health Center and/or the CSU, Chico University Police, if an individual's health or safety appears to be in jeopardy;

Office of Employment Practices and Affirmative Action, if violations occur in the course of employment and/or in instances of sexual harassment (ext. 4666);

Campus [agent to receive notification](#) of a claimed copyright infringement, as it relates to the Digital Millennium Copyright Act of 1998 (ext. 6212);

Information Resources, serving campuswide resources, if an incident potentially bears external or legal consequences for the institution. This office is available to assist with investigations, generally under the

auspices of the college/unit policy officer. You may also contact this office if you wish to report an incident but are unable to do so through normal channels (ext. 6212);

Questions related to the 4CNet policy can be sent to aup@4c.net;

Additional information about copyrights can be found at

[TLP's List of Copyright Information Web Sites](#)

[Meriam Library's Copyright Information Page](#)

Notification

The University will disclose this policy to new users at the time of their initial connection to the network by providing them with a copy of this document. Each semester a reminder will be sent to all users through the faculty/staff and student email Announcements, referencing the web location of the full text of the policy. It is the responsibility of the user to read and comply with this policy.