Interim Acceptable Use Policy of Information Technology Resources
California State University, Fresno

1. Policy

California State University, Fresno (University) is responsible for overseeing the appropriate use of its information technology resources and requires individuals accessing and using the University's resources to adhere to the rules for responsible and appropriate use of such resources.

2. Reason

The University encourages the use of information technology resources to share information and knowledge in support of its mission of education, research, public service, and to conduct the University's business. This policy provides a framework to promote and encourage responsible use of information technology resources.

3. Scope

All staff, faculty, and students of the University, guests, auxiliary organizations, third parties, and any other entities granted access or using any University information technology resource must adhere to this policy.

Information technology resources (information resources) are devices or technologies that are designed, built, operated, organized, or maintained to process, store, transmit, or output information. These information resources include, but are not limited to, voice, data and video networks, computer accounts, electronic communications, files, computing facilities, laboratories, software, and data.

4. Guiding Principles

The University recognizes the principles of academic freedom and shared governance, freedom of speech, and privacy rights that hold important implications for the use of information resources. This policy reflects these principles within the context of the University's legal and other obligations.

The University's information resources 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, staff, and those members accessing resources are responsible for seeing that these information resources are used in an effective, efficient, ethical, and lawful manner.

5. Rights and Responsibilities

University information resources provide access to resources on and off campus, as well as the ability to communicate worldwide. This open access is a privilege requiring individuals to use information resources responsibly. Access and use of information resources carries with it certain conditions and responsibilities.

Individuals shall respect the rights of other users, respect the integrity of the information resources and observe all applicable laws, regulations, executive orders, collective bargaining agreements, policies, and contractual obligations. Individuals must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws. When accessing external resources to the University, individuals are responsible for abiding by any policies, rules, and codes of conduct applying to such resources.

Individuals are responsible for the proper use of information resources assigned to them, including accounts, passwords, computers and data. Individuals shall not knowingly falsely identify themselves and will take steps to correct misrepresentations if they have falsely or mistakenly identified themselves.

Misuse of these resources or violation of the delineated conditions in this policy may result in the termination of the accounts and access, or, in cases of more serious infractions, the submission of the case to an appropriate disciplinary authority for further investigation.

Individuals should report any apparent violations of law, university policy, and college/school or department policy concerning the acceptable use of information resources to their appropriate university manager and/or the Chief Information Security Officer (see section 11).

6. Privacy

The University's intent is to consider information and content as private and confidential unless they have explicitly been made available to other authorized individuals. It is not the University's practice to inspect, monitor or disclose the content of information stored on or transmitted through the University's information resources.

However, individuals should not expect privacy in their access and use of University information resources. As a practical matter, authorized individuals may access others' information and/or electronic communication when necessary for the maintenance and security of university information resources and services. When performing these functions, every effort is made to ensure the privacy of an individual's information. However, if violations are discovered, they will be handled through normal university procedures.

Other causes for inspection, monitoring, and disclosure include the need to ensure operational effectiveness of resources and services; prevent or investigate a suspected breach of the law, this policy, or other University policies; or as part of an official University disciplinary action, court enforced subpoena, search warrant, or valid requests under the California Public Records Act.

In addition, electronic communication is neither private nor secure. In communicating via e-mail, instant messaging, or other forms, it is the individual and not the University, who assumes responsibility for its contents. All electronic messages may be subject to discovery in civil litigation or in criminal investigations. In most instances, there is no reason for electronic messages to be retrieved by anyone other than the intended addressee, but in limited and appropriate circumstances (e.g., in course of an official investigation of wrongdoing), electronic communication may become subject to internal monitoring by an authorized individual.

7. Copyright, Licensing, and Related Concepts

Among other rights, copyright law, in general, gives the owner of a piece of literary or associated work (including, amongst other types of work, software, music, videos, games, artistic works, and photographs) the right to prevent that work from unauthorized copying and distribution via any form. As the University is subject to federal law, students, staff, faculty, and administrators must comply and abide with copyright law and University copyright policy.

The concept of 'fair use' allows limited use of copyright works for the purposes of research, private study, criticism and review; since the 'fair use' test is qualitative rather than quantitative, the prospective individual may need to check with the copyright owner before use.

This means that most information and software is subject to copyright and/or restrictions on its use. Each individual must respect this copyright and must comply with published usage restrictions relating to any program, information, image, web page, or other material. Any individual who installs software and/or information on University resources must ensure full compliance with any relevant copyright requirements and licensing agreements.

8. Legal Requirements

Law prohibits the unauthorized access, modification, interference, or disruption of information resources, the harassment of individuals via electronic methods, and other inappropriate actions involving the use of information resources[1]. Violations of law may be subject to penalties under civil or criminal code. University policies on sexual or other forms of harassment apply fully to all information resources, including electronic communication and the Internet.

University information resources shall never be used for purposes intended to incite or commit a crime; for example, it is illegal to post a credit card number, copyrighted information, or a computer password. Criminal and illegal use may include obscenity, child pornography, threats, harassment, theft, and unauthorized access.

University information resources such as electronic communication (e.g. e-mail, voice mail, instant messaging, etc.) are provided for university-related activities. Fraudulent, harassing, or obscene messages and/or materials are not to be printed, sent, or stored. No e-mail or message shall be created or sent, nor Web pages created, that may constitute intimidating, hostile, or offensive material based on gender, race, color, religion, national origin, sexual orientation, or disability. The University's policies on sexual or other forms of harassment apply fully to electronic communication and the Internet.

The following acts are relevant to use of information resources in a university setting. Violations may incur sanctions by the University and/or legal proceedings. Examples of violations, given below, are not intended to cover all eventualities:

a. Knowingly gaining or attempting to gain unauthorized access to any information resource, program, or information that the individual has no authorization to access or use.
b. Intentionally gaining or attempting to enable inappropriate levels of access.
c. Sharing the user name and password of his/her account without authorization and the explicit agreement by each party (lender and borrower).
d. Unauthorized modification or access to any program, file, data, electronic communication, or other computer material belonging to another individual or organization.
e. Using information resources to impersonate, harass, threaten, or otherwise cause harm to other individuals or organizations.
f. Intentionally transmitting any computer virus, worm, or other malicious software.
g. Taking actions threatening the security or capacity of information resources or which modify, destroy, damage, or overload these resources.
h. Violating any applicable law, university policy, executive order, or contractual obligation.

9. Prohibited Use

The University is a not-for-profit, tax-exempt organization and is subject to applicable federal and state laws and regulations on the use of University property. Any use of information resources in a manner that places the University in jeopardy of such status is prohibited. University information resources shall not be used for non-University commercial purposes, except as permitted under University policy or with appropriate approval.

University information resources (e.g., computer facilities, laboratories, offices, the library, etc.) do not provide a private environment for accessing electronic communication or other resources. Therefore, individuals 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, may be seen to have a strong possibility of creating a hostile environment for other students, faculty, staff, and visitors.

[1] Reference California Penal Code 502 & 18 U.S.C. § 1030

University information resources shall not be used to imply University endorsement, including the support or opposition of the University with regard to any religious or political activity or issue. University resources shall not be used for mass messaging to newsgroups, bulletin boards, mailing lists,, or other individuals. Individuals shall not imply University endorsement of products or services of a non-University entity from a University information resource, without approval. Individuals shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the University unless authorized to do so. To avoid this, individuals may use a disclaimer such as "The opinions or statements expressed herein should not be taken as a position of or endorsement by California State University, Fresno."

University resources shall not be used to store, distribute, or transmit obscene or offensive material. No individual may hold in files (or Web pages), or transmit electronically, information, which constitutes obscene or offensive material. In this context, the individual is responsible for the content of his/her files, Web pages and messages. Any such data received involuntarily, e.g., through electronic mail, should be deleted. These aforementioned restrictions might not prohibit such access or retention of such materials if they are being used for a specific academic purpose.

10. Incidental Use

Information resources are owned and operated by the University and/or its various schools, colleges, departments, auxiliary organizations, programs, recognized student and campus organizations, and are to be used for university-related activities and occasional incidental use. Such resources are provided to facilitate a person's essential work as an employee, student, or other role within the University. Individuals may use University information resources for occasional incidental personal purposes of a private nature if such use does not:

a. Interfere with the University's operation of its information resources.
b. Burden the University with noticeable incremental costs.
c. Interfere with a person's employment or other obligations to the University.
d. Constitute or result in financial gain.
e. Involve accessing, creating, downloading, or disseminating any information that a reasonable person would deem inappropriate, such as pornography or racist materials.
f. Violate any applicable law, university policy, executive order, or contractual obligation.

11. Reporting

Suspected violations of this policy should be reported electronically at security@csufresno.edu or to the

Chief Information Security Officer
Information Technology Services
2225 East San Ramon Avenue
Mail Stop MF93
Fresno, CA. 93740-8029
Phone: (559) 278-3923

12. Enforcement

Federal and state laws and University policies in some cases apply specifically to the use of information resources. In other cases, they may apply generally to personal conduct in which the use of information resources is incidental. Violations of law may be referred for legal action.

Violations of provisions in this policy will be handled through normal University procedures. Violators may be subject to disciplinary action up to and including dismissal or expulsion under applicable University policies and collective bargaining agreements.

Cases of more serious infractions will be submitted 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).

The University reserves the right to terminate, suspend, and/or limit access to its information resources when policies or laws are violated and to use appropriate means to ensure continued service delivery at all times, preserve network/system integrity, and safeguard its information resources.

Approved as an Interim Policy by President Welty on February 21, 2008