San José State
UNIVERSITY

A campus of The California State University

Office of the Academic Senate • One Washington Square • San Jose, California 95192-0024 • 408-924-2440 • Fax: 408-924-2451

S02-8

At its meeting of May 13, 2002, the Academic Senate passed the following Policy Recommendation presented by Ken Peter for the Executive Committee.

POLICY RECOMMENDATION
INFORMATION TECHNOLOGY RESOURCES RESPONSIBLE USE POLICY

Whereas: The CSU requires each campus to have a policy on responsible use of information technology resources and SJSU does not currently have such a policy, and

Whereas: Appropriate use of campus technology resources is crucial to course delivery, communication, administrative activities, and delivery of employee and student services, thus necessitating responsible usage of the technology, and policies and procedures to avoid misuse, and

Whereas: The University Information Technology Board drafted an acceptable use policy to present to the Executive Committee who now forward the policy to the Academic Senate for its consideration; therefore be it

Resolved: That we acknowledge and thank Cal Poly San Luis Obispo for providing us the framework for the policy, be it further

Resolved: That the following Information Technology Resources Responsible Use Policy be adopted and implemented as soon as possible, but no later than August 24, 2002, be it further

Resolved: That the policy be posted to the University's web page, as well as those of the University Computing & Telecommunications and Academic Technology units, with conventional indexing techniques that include keywords such as "acceptable use" to facilitate search and retrieval, be it further

Resolved: That all departments, colleges and divisions be given copies of the policy and encouraged to add a link to their web site where appropriate so that users of campus technology resources will have ready access to the policy, be it finally

Resolved: That the Information Technology Board be charged with drafting general guidelines to assist the campus in implementing and complying with this policy and forwarding to the Senate those guidelines for Senate approval via the Executive Committee.

Information Technology Resources Responsible Use Policy

Table of Contents

A. Scope

This policy applies to any user of the University's information technology resources, whether initiated from a computer located on or off-campus. This includes any computer and information system or resource, including means of access, networks, and the data residing thereon. This policy applies to the use of all University information technology resources whether centrally-administered or locally-administered. Administrators of individual or dedicated University resources may enact additional policies or create guidelines specific to those resources provided they do not conflict with the provisions of this and other official San José State University policies and laws. Users are subject to both the provisions of this policy and any policies specific to the individual systems they use. In matters in which there is a discrepancy between local unit/or state and federal policy and this policy, the issues in dispute will be reviewed by the IT Board or during times where a quorum of the IT Board is not available, members of the Executive Committee may act for the IT Board.

B. Purpose

This policy is not intended to prevent or prohibit the sanctioned use of campus resources as required to meet SJSU's core mission and academic and administrative purposes. The principal concern of this responsible use policy is the effective and efficient use of information technology resources. The primary focus is to insure that the resources are used in a manner that does not impair or impede the use of these resources by others in their pursuit of the mission of the University. This policy is intended to ensure

1. the integrity, reliability, and good performance of University resources;
2. that the resource-user community operates according to established policies and applicable laws;
3. that these resources are used for their intended purposes; and
4. that appropriate measures are in place to assure the policy is honored.

The policy is intended to permit, rather than proscribe, reasonable resource-user access within institutional priorities and financial capabilities.

This policy is intended to promote and encourage responsible use while minimizing the potential for misuse and not imposing broad-based restrictions on all users. Users of IT resources should consult the resource provider for any additional guidelines and limitations that may be in place for the unit or associated organization, eg. Library, Housing, Associated Students, etc.

C. Guiding Principles

The following principles underlie this policy and should guide its application and interpretation:

1. Freedom of thought, inquiry, and expression is a paramount value of the SJSU community. To preserve that freedom, the community relies on the integrity and responsible use of University resources by each of its members.
2. The President is ultimately responsible for implementation of this policy, but may delegate this responsibility. For any policy issue relating to this policy the President should seek consultation with the Academic Senate.

3. Information technology resources are provided to support the University's mission of education, research and service. To ensure that these shared and finite resources are used effectively to further the University's mission, each user has the responsibility to:

   a. use the resources appropriately and efficiently;

   b. respect the freedom and privacy of others;

   c. protect the stability and security of the resources; and

   d. understand and fully abide by established University policies and applicable public laws.

4. Responsible use of University resources will be given priority over the current or potential design, capability or functionality of specific information technology resources including operating systems, hardware, software, and the Internet.

5. Users of information technology resources are expected to uphold the highest academic standards in accordance with the Students Rights and Responsibilities Policy (S90-5), Academic Freedom and Professional Responsibilities (S99-8), Privacy of Electronic Information and Communications (F97-7), and other applicable University policies and practices.

D. Policy Application

As a general guideline, the institution regards the principle of academic freedom to be a key factor in assuring the effective application of this policy and its procedures and practices. State and federal laws must also be considered. The University's role in supporting or acting to enforce such law is also critical to how this policy will be applied.

1. All existing laws (federal, state and local) and State of California, California State University and SJSU regulations and policies apply, including not only laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. This may also include laws of other states and countries where material is accessed electronically via University resources by users within those jurisdictions or material originating within those jurisdictions is accessed via University resources.

2. The accessibility of certain University information technology resources, such as network-based services, implies a degree of risk that the existence, viewing or receipt of such information/content may be offensive. As a matter of policy, the University protects expression by members of its community and does not wish to become an arbiter of what may be regarded as "offensive" by some members of the community. However, in exceptional cases, the University may decide that such material directed at individuals or classes of individuals presents such a hostile environment under the law that certain restrictive actions are warranted.

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

includes monitoring routing information of communications across its network services and transaction records residing on University resources, scanning systems attached to the SJSU network for security problems, disconnecting systems that have become a security hazard, and restricting the material transported across the network or posted on University systems. This level of action is considered one of last resort and would be imposed only when other means of remedy are unsuccessful or are prevented due to timing constraints. If possible, the University will give notification to the affected units of a shutdown and give reasons why the shutdown has occurred. These types of actions will be reported to the University IT Board each semester for its review. Appeals in writing will be considered by the University Information Technology Board or, in summer, the Executive Committee of the Senate.

4. Hyperlinks within the policy to external documents are provided for the reference and convenience of readers. They should not be viewed as implying that the referenced document is being incorporated into this policy except as stated or otherwise specified in the policy itself.

E. Policy Provisions

This section is not intended to provide a full accounting of applicable laws and policies. Rather, it is intended to highlight major areas of concern with respect to responsible use of SJSU resources and specific issues required by law or CSU policy to be included.

1. Authorized Use / Access

Access to SJSU's information technology resources is a privilege granted to faculty, staff and students in support of their studies, instruction, duties as employees, official business with the University, and/or other University-sanctioned activities. Access may also be granted to individuals outside of SJSU for purposes consistent with the mission of the University.

With the exception of implicitly publicly accessible resources such as websites, access to SJSU information technology resources may not be transferred or extended by members of the University community to outside individuals or groups without prior approval of faculty, staff or administrator. Such access must be limited in nature and fall within the scope of the educational mission of the institution. The authorizing University official is expected to ensure that such access is not abused.

Gaining access to the University's information technology resources does not imply the right to use those resources. The University reserves the right to limit, restrict, remove or extend access to and privileges within, material posted on, or communications via its information technology resources, consistent with this policy, applicable law or as the result of University disciplinary processes, and irrespective of the originating access point.

It is expected that these resources will be used efficiently and responsibly in support of the mission of the University as set forth in this policy. All other use not consistent with this policy may be considered unauthorized use.

2. Data Security, Confidentiality and Privacy

SJSU users are responsible for ensuring the confidentiality and appropriate use of institutional data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students, faculty and staff concerning the use and release of personal information, as required by law or existing policies.

Electronic mail and computer files are considered private to the fullest extent permitted by law and University policy (Privacy of Electronic Information and Communications Policy (F97-7). Access to such files will generally require permission of the sender/recipient of a message or the owner of the account in which the material resides, court order, or other actions defined by law or University policy. However, in the event of a sanctioned University investigation for alleged misconduct, e-mail or files may be locked or copied to prevent destruction and loss of information. Users may employ methods to increase the privacy of their files, provided they do not violate any provision of this policy or degrade system/network performance.

All users of SJSU's information technology resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or restricted access to such information. SJSU strives to provide the highest degree of security when transferring data, but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

3. Electronic Information Retention and Disclosure

Original electronic materials on central computing equipment and/or copies may be retained for specified periods of time on system backups and other locations; however the University does not warrant that such information can be retrieved.

Unless otherwise required by law and/or policy, SJSU reserves the right to delete stored files and messages to preserve system integrity. Except in an emergency, users will be given ample advance notice, taking the academic year calendar into account, to save any personal files and messages.

Electronic files or messages, whether or not created and stored on University resources, may constitute a University record subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. Electronic copies must be provided in response to a public record request or legally issued subpoena, subject to very limited exceptions, as with other documents created and retained by the University.

Disclosure of confidential information to unauthorized persons or entities, or the use of such information for self-interest or advantage, is prohibited. Access to non-public institutional data by unauthorized persons or entities is prohibited.

Requests for disclosure of confidential information and retention of potential evidence will be honored when approved by authorized University officials or required by state or federal law.

4. Network and System Integrity

In accordance with California State Penal Code Section 502, CSU's 4Cnet Acceptable Use Policy and other policies and laws, activities and behaviors that threaten the integrity of computer networks or systems are prohibited on both University-owned and privately-owned equipment operated on or through University resources. These activities and behaviors include, but are not limited to:

1. Intentional or careless interference with or disruption of computer systems and networks and related services, including but not limited to the propagation of computer "worms," "viruses" and "Trojan Horses" and other activities that could have a negative impact on the SJSU computing environment in the judgment of the Associate Vice President, University Computing and Telecommunications or designee.

2. Intentionally or carelessly performing an act that places an excessive load on a computer or network to the extent that other users may be denied service or the use of electronic networks or information systems may be disrupted

3. Failure to comply with authorized requests from designated University officials to discontinue activities that threaten the operation or integrity of computers, systems or networks

4. Negligently or intentionally revealing passwords or otherwise permitting the use by others of University-assigned accounts for computer and network access. Individual password security is the responsibility of each user. The user is responsible for all uses of their accounts, independent of authorization.

5. Altering or attempting to alter files or systems without authorization

6. Unauthorized scanning of ports, computers and networks

7. Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities

8. Connecting unauthorized equipment to the campus network or computers. University authorized business and other activities directly related to the academic mission of the University are excluded.

9. Attempting to alter any University computing or network components, including but not limited to bridges, routers, hubs, wiring, and

connections, without authorization or beyond one's level of authorization as designated by the administrator responsible for that equipment, ie. the Associate Vice President, University Computing and Telecommunications, or unit Dean or designee.

10. Utilizing network or system identification numbers or names that are not assigned for one's specific use on the designated system

11. Using campus resources to gain unauthorized access to any computer system and/or using someone else's computer without their permission

12. Providing services or accounts on University computers or via University networks to other users from a personal computer unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements. University authorized business and other activities directly related to the academic mission of the University, are also excluded.

13. Registering a SJSU IP address with any other domain name for other than university business.

5. Commercial Use

Use of the University's information technology resources is strictly prohibited for unauthorized commercial activities, personal gain, and private, or otherwise unrelated to the University, business or fundraising. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling University resources.

Campus auxiliary organizations are authorized to provide services and products to students, faculty and staff, and invited guests of the University through operating and service support leases. The University President or designee may authorize additional limited commercial uses under separate policy provisions. Such uses are excepted from the above prohibitions. These prohibitions are not intended to infringe on authorized uses that enable students, staff and faculty to carry out their duties and assignments in support of the University mission.

6. Fraud

Use of University information technology resources for purposes of perpetrating fraud in any form is strictly prohibited. Fraudulent activities include but are not limited to sending any fraudulent electronic transmission, fraudulent requests for confidential information and fraudulent submission and/or authorization of electronic purchase requisitions.

7. Political Campaigns:

California Government Code 8314 prohibits the use of state resources for major political campaign activity. This provision does not apply to political activities related to on-campus student government, including the conduct of student elections, or student club activities and sponsored events conducted with prior approval of the University. It does not apply to individual student activities, e.g., websites, which constitute free speech. It does not apply to incidental and minimal use of state resources. Such activities must comply with all other provisions of this policy, including the section on electronic communications, when using University resources.

8. Harassment

Harassment of others via electronic methods is prohibited under California State Penal Code Section 653m, other applicable laws and University policies. It is a violation of this policy to use electronic means to harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference. It may be a violation of this policy to use electronic means to harass or threaten groups of individuals by creating a hostile environment.

9. Copyright and Fair Use

Federal copyright law applies to all forms of information, including electronic communications, and violations are prohibited under this policy. Infringements of copyright laws include, but are not limited to, making unauthorized copies of any copyrighted material (including software, computer code, text, images, audio, and video), and displaying or distributing copyrighted materials over computer networks without the author's permission except as provided in limited form by copyright fair use restrictions. The "fair use" provision of the copyright law allows for limited reproduction and distribution of published works without permission for such purposes as criticism, news reporting, teaching (including multiple copies for classroom use), scholarship, or research. The University will not tolerate academic dishonesty (s98-1) or theft of intellectual property in any form.

10. Trademarks and Patents

Student, faculty and staff use of University information technology resources in the creation of inventions and other intellectual property that may be patented, trademarked or licensed for commercial purposes must be consistent with SJSU's Intellectual Property Policy (F98-3). Unauthorized use of patents, trade secrets and trademarked names or symbols is prohibited. Use of SJSU's name and symbols must comply with University policy.

11. Electronic Communications

University electronic communications are to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences, to facilitate the effective business and administrative processes of the University, and to foster effective communications within the academic community. Electronic mail, news posts, chat sessions or any other form of electronic communication must comply with SJSU's Privacy of Electronic Information and Communications Policy (F97-7).

12. Web Sites

An official SJSU web page is one that is formally acknowledged by the chief officer of a University department or division as representing that entity accurately and in a manner consistent with SJSU's mission. Without such acknowledgment, a web site, regardless of content, is not "official." Official pages are the property and responsibility of the divisions that create them and follow the University Web Style Guide and University Logo Guidelines

"Unofficial" information may also be posted and maintained by individual students, faculty, staff and student organizations. SJSU does not undertake to edit, screen, monitor, or censor information posted by unofficial authors, whether or not originated by unofficial authors or third parties, and does not accept any responsibility or liability for such information even when it is conveyed through University-owned servers.

Both official and unofficial web sites are subject to the other provisions of this policy if they use University resources such as University-owned servers and the SJSU network to transmit and receive information.

F. Policy Compliance

The University Information Technology Board is authorized by the President to ensure that the appropriate processes to administer the policy are in place, communicated and followed by the University community. The President or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate University officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

The President or designee will inform users about the policy; receive and respond to complaints; collect and secure evidence as required; advise and assist University offices on the interpretation, investigation and enforcement of this policy; consult with University Legal Counsel on matters involving interpretation of law, campus policy, or requests from outside law enforcement agencies and/or legal counsel; and maintain a record of each incident and its resolution to inform future policy changes.

G. Consequences of Non-Compliance

Enforcement will be based upon receipt by University Computing and Telecommunications of one or more formal complaints about a specific incident or through discovery of a possible violation in the normal course of administering information technology resources.

First offense and minor infractions of this policy, when accidental or unintentional, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the resource. This may be done through e-mail or in-person discussion and education.

Repeated offenses and serious incidents of non-compliance may lead to University disciplinary action under CSU and University disciplinary policies and procedures for students and employees, employee contract provisions where appropriate, private civil action, and/or criminal charges. Serious incidents of non-compliance include but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior.

In addition to the above, inappropriate use of information technology resources may result in personal criminal, civil and other administrative liability.

Appeals of University actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for SJSU students and employees.

H. Reporting Irresponsible or Inappropriate Use

The President or designee is responsible for reviewing violations of this policy and will act in accordance with campus policies and guidelines for investigations and resolution of problems. Suspected infractions of this policy should be reported to University Computing and Telecommunications at nettel@sjsu.edu.

Any employee may report a violation of this policy. The infraction must be reported to their immediate superior who may take those actions that are appropriate under this policy. There might be situations when the following additional offices/officials should be notified of suspected violations when filing a complaint:

- **Supervisors, Department Heads, Deans, Program Administrators** and/or one of the following offices if the incident occurs in the course of employment with the University:

  Human Resources - (408) 924-2250

  Faculty Affairs - (408) 924-2450

- **Student Records -** (408) 924-2550 - If the incident involves inappropriate use of SJSU student information. The Records Office is responsible for investigating reports of Family Educational Rights and Privacy Act of 1974 (FERPA) violations and maintaining records for the Department of Education.

- **Judicial Affairs –** (408) 924-5985 - If the incident involves student misconduct.

- **University Computing and Telecommunications –** (408) 924-2340 - If the incident involves inappropriate access to or use of institutional data.

- **SJSU University Police** - 911 for emergencies - If an individual's health and safety appears to be in jeopardy or a violation of law may be involved, or (408) 924-2223 for non-emergency situations.

I. Policy Review and Practices Oversight

The President or designee is responsible for application and enforcement of this policy. The University Information Technology Board shall review this policy on an annual basis or as the need arises, make recommendations for any changes, and provide oversight and periodic review of the practices used to implement this policy. Recommended changes shall be reviewed and approved by the President or designee in consultation with the Academic Senate. The current version of the policy will be posted and maintained on the SJSU web site. A printed copy will be available at the University Library Reference Desk. The committee chair will make an annual written report to the Senate reporting actions of the committee taken throughout the year.

ACTION BY UNIVERSITY PRESIDENT: APPROVED BY PRESIDENT ROBERT CARET ON JUNE 5, 2002.