

ACADEMIC SENATE
Of
CALIFORNIA POLYTECHNIC STATE UNIVERSITY
San Luis Obispo, CA

AS-554-01/IACC
RESOLUTION ON INFORMATION TECHNOLOGY RESOURCES
RESPONSIBLE USE POLICY

- 1 WHEREAS, Information technology resources are a finite shared resource provided to students, faculty, and
2 staff to support Cal Poly's mission of education, research, and service; and
3
4 WHEREAS, The University is accountable for ensuring that its resources are used responsibly; and
5
6 WHEREAS, A clear and comprehensive policy is needed to inform the campus community about appropriate
7 use and to enable the University to act when misuses occur; and
8
9 WHEREAS, An interim policy has been in effect since the start of Fall Quarter 2000 and is posted on the Cal
10 Poly web site at <http://its.calpoly.edu/Policies/RUP-INT/>; and
11
12 WHEREAS, The policy incorporates existing University, CSU, and state policies as well as federal and state
13 laws, reflects best practices from other universities, and provides specific examples of appropriate
14 and inappropriate uses; and
15
16 WHEREAS, The policy recognizes and respects academic freedom, freedom of expression, and the right to
17 privacy of individual users wherever possible; and
18
19 WHEREAS, The policy uses established University processes to address alleged violations by Cal Poly
20 students, faculty, and staff; and will be reviewed and updated at least annually to reflect changes in
21 policy, the law, and technology; and
22
23 WHEREAS, Endorsement of the Responsible Use Policy does not imply endorsement by the Academic Senate
24 of other policies referenced therein; and
25
26 WHEREAS, Information Technology Services will consult with the Academic Senate and other campus
27 constituent groups on substantive changes to this policy and on the development of related
28 information technology policies and practices; and
29
30 WHEREAS, The Instructional Advisory Committee on Computing (IACC), Administrative Advisory
31 Committee on Computing (AACC), and Information Resources Management Policy and Planning
32 Committee (IRMPPC) have endorsed the policy and recommended that it be adopted and
33 implemented by the University; therefore, be it
34
35 RESOLVED: That the Academic Senate endorse the Information Technology Resources Responsible Use Policy
36 and recommend that it be adopted and implemented by the University; and be it further
37
38 RESOLVED: Modifications and/or updates to the Responsible Use Policy (RUP) be brought before the
39 Instructional Advisory Committee on Computing (IACC) and the Academic Senate be informed of
40 all approved changes to the RUP.

Proposed by: Instructional Advisory Committee on Computing (IACC)
Date: October 23, 2000
Revised: February 5, 2001

Information Technology Resources Responsible Use Policy (Interim)

Revised ~~November, 2000~~ February 2001

Table of Contents

A.	Scope	2
B.	Purpose	2
C.	Guiding Principles	2
D.	Policy Application	3
E.	Policy Provisions	
1.	Authorized <i>Use/Access</i>	3
2.	Data Security, Confidentiality and Privacy	4
3.	Electronic Information Retention and Disclosure	4
4.	Network and System Integrity	5
5.	Commercial Use	6
6.	Political Advocacy	6
7.	Harassment	7
8.	Copyright and Fair Use	7
9.	Trademark and Patents	7
10.	Electronic Communications	7
11.	Web Sites	7
F.	Policy Compliance	8
G.	Consequences of Non-Compliance	8
H.	Reporting Irresponsible or Inappropriate Use	9
I.	Policy Review and Practices Oversight	9
J.	Glossary and Definition of Terms	9
	<i>Appendix A</i> - http://its.calpoly.edu/IPoliciesIRUP-INT/define.doc	
K.	Specific Examples of Responsible and Irresponsible Use	9
	<i>Appendix B</i> - http://its.calpoly.edu/IPoliciesIRUP-INT/example.doc	
L.	References and Works Cited	9
	<i>Appendix C</i> - http://its.calpoly.edu/IPoliciesIRUP.INT/refer.doc	
M.	Policy Implementation and Practices	9
	<i>Appendix D</i> - http://its.calpoly.edu/IPoliciesIRUP-INT/practice.doc	

Information Technology Resources Responsible Use Policy (Interim)

Revised ~~November, 2000~~ February 2001

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 specific to those resources provided they do not conflict with the provisions of this and other official policies and laws. Users are subject to both the provisions of this policy and any policies specific to the individual systems they use.

B. Purpose

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.

This policy is not intended to prevent or prohibit the sanctioned use of campus resources as required to meet Cal Poly's core mission and academic and administrative purposes.

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 Cal Poly community. To preserve that freedom, the community relies on the integrity and responsible use of University resources by each of its members.
2. 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.
3. 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.
 4. Users of information technology resources are expected to uphold the highest academic standards in accordance with the Campus Code of Conduct and other 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. The law is another source of guidance. 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 Cal Poly 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 Cal Poly 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.
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 Cal Poly resources and specific issues required by law or CSU policy to be included.

1. Authorized Use / Access

Access to Cal Poly'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 Cal Poly for purposes consistent with the mission of the University.

With the exception of implicitly publicly accessible resources such as websites, access to Cal Poly information technology resources may not be transferred or extended by members of the University community to outside individuals or groups without prior approval of an authorized University official. 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

Cal Poly 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, including the Confidentiality-Security Policy and Policy on the Use and Release of Student Information.

Electronic mail and computer files are considered private to the fullest extent permitted by law. 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. 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 Cal Poly'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. Cal Poly

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 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, Cal Poly reserves the right to delete stored files and messages to preserve system integrity. Except in an emergency, users will be given advance notice to delete 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 (Government Code 6250-6270 and 6275-6277) 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 in connection with alleged misconduct will be honored when approved by authorized University officials or required by law.

4. Network and System Integrity

In accordance with California State Penal Code Section 502, Cal Poly's Computer Crimes Policy, CSU's 4Cne1 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:

H-1. 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"

H-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

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

H-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 loopholes
- ¶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 g. Attempting to alter any University computing or network components without authorization or beyond one's level of authorization, including but not limited to bridges, routers, hubs, wiring, connections, etc.
- ¶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 Cal Poly IP address with any other domain name

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.

(Detailed guidelines are being developed to clarify exceptions to this provision and will be incorporated or referenced in the next major revision.)

6. Political Advocacy

It is generally inappropriate for individual employees to use University resources to engage in political advocacy in election campaigns. State law generally prohibits the use of public funds for this purpose and Government Code Section 8314 makes it illegal for any state employee or consultant to use or permit others to use state resources for any campaign activity not authorized by law.

An employee can be held personally liable for intentionally or negligently violating Government Code Section 8314 for up to \$1,000 per day the violation occurs plus three times the value of the unlawful use of state resources. Due to the personal

nature of this activity, the State of California would not indemnify or defend the employee if an action was pursued against them for violating this statute.

The courts have yet to address the specific issue of whether an individual's use of state supported e-mail for political purposes violates the law. While the University may choose not to be involved in deciding whether a personal communication violates this provision, other policy provisions may apply and an employee may still be subject to personal liability under the law. Employees should exercise appropriate caution prior to engaging in such activities, which may have negative consequences for them and the University.

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. Such activities must comply with all other provisions of this policy, including the section on electronic communications, when using University resources.

7. 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.

8. 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, 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. For more information on this issue, see Stanford University's Copyright and Fair Use website. The University will not tolerate academic cheating, plagiarism or theft of intellectual property in any form.

9. 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 Cal Poly's Intellectual Property Policy. Unauthorized use of trade secrets and trademarked names or symbols is prohibited. Use of Cal Poly's trademarked name and symbols must comply with University policy.

10. 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 Cal Poly's Electronic Mail Policy.

11. Web Sites

An official Cal Poly 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 Cal Poly'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.

"Unofficial" information may also be posted and maintained by individual students, faculty, staff and student organizations. Cal Poly 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 Cal Poly network to transmit and receive information.

F. Policy Compliance

The Vice Provost/Chief Information Officer 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 Vice Provost/Chief Information Officer 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 Vice Provost/Chief Information Officer 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 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 offenses 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 formal disciplinary actions under CSU and University disciplinary policies and procedures for students and employees and employee contract provisions where appropriate. 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 materials, 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 Cal Poly students and employees.

H. Reporting Irresponsible or Inappropriate Use

Suspected infractions of this policy should be reported to Information Technology Services at abuse@calpoly.edu or complaints@calpoly.edu in accordance with [Appendix D, Policy Implementation and Practices](#). There might be situations when the following additional offices/officials should be notified of suspected violations when filing a complaint:

- Supervisors, Department Heads/Chairs, Deans, Program Administrators and/or one of the following offices if the incident occurs in the course of employment with the University:
 - [Human Resources and Employment Equity](#) (State) - (805) 756-2236
 - [Academic Personnel](#) (Faculty Affairs) - (805) 756-2844
 - Human Resources (ASI) - (805) 756-1281
 - Human Resources (Foundation) - (805) 756-1121
- [Academic Records](#) - If the incident involves inappropriate use of Cal Poly student information. The registrar is responsible for investigating reports of [Family Educational Rights and Privacy Act of 1974 \(FERPA\)](#) violations and maintaining records for the Department of Education. (805) 756-2531
- [Information Security Officer/Risk Manager](#) - If the incident involves inappropriate access to or use of institutional data. (805) 756-6755
- Cal Poly University Police - If an individual's health and safety appears to be in jeopardy or a violation of law may be involved. (805) 756-2281 or 911 (Emergency)

I. Policy Review and Practices Oversight

The Vice Provost for Information Technology/Chief Information Officer is responsible for application and enforcement of this policy. The Acceptable Use Policy sub-Committee (AUPC) of the Information Resources Management Policy and Planning Committee (IRMPPC) 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 Vice Provost/Chief Information Officer in consultation with the IRMPPC and the President. The current version of the policy will be posted and maintained on the Cal Poly web site. A hard copy will be available at the Kennedy Library Reserve Desk.

J. Glossary and Definition of Terms

Appendix A - <http://its.calpoly.edu/IPolicies/IRUP-INT/define.doc>

K. Specific Examples of Responsible and Irresponsible Uses

Appendix B - <http://its.calpoly.edu/IPolicies/IRUP-INT/example.doc>

L. References and Works Cited

Appendix C - <http://its.calpoly.edu/IPolicies/IRUP-INT/refer.doc>

M. Policy Implementation and Practices

Appendix D - <http://its.calpoly.edu/IPolicies/IRUP-INT/practice.doc>

Information Technology Resources Responsible Use Policy (Interim)

Appendix B Specific Examples of Responsible and Irresponsible Uses

Appropriate Uses

Authorized Use

- A student working with a professor uses University computers to set up a web page for his senior project.
- A student, faculty or staff member uses their University account to set up an "unofficial," personal web page with pictures from their summer vacation.
- A student browses web sites not directly related to their role at the University.
- A very ill student gives their password to another student to check e-mail on their behalf.
- A staff member away from campus delegates another staff member to read and respond to e-mail and calendar items in their absence. They provide their login ID and password to the same staff member to permit others to access files in their absence.
- A Cal Poly staff member uses the Cal Poly network to "telecommute" from home.
- Students in a class use a single ID and password to access shared course materials and to complete class assignments. The professor uses the same ID and password to review completed assignments and post new materials.

Network/System Integrity

- A student sets up a web site on their computer in the residence halls and grants permission to other users to download via Cal Poly's network some audio/video clips that he created.
- A student makes an intra-campus file transfer to a designated computer in order to share a file that one or more students are using in a class.
- A student creates user accounts on their own computer to allow access to shared files for a group project via the Cal Poly network.
- A student resident runs a web server on their own computer that provides pictures of a recent trip to Tahoe.
- A student uses the Cal Poly network to play online games provided other network users are not adversely impacted.
- A network administrator conducts a port scan of the computers attached to that network.

Commercial Use

- A faculty member uses their Cal Poly e-mail account to communicate with a publisher about a textbook they are developing for a course they teach.

Information Technology Resources Responsible Use Policy (Interim)

- Posting a notice about items for sale to a newsgroup intended for that purpose or to an off-campus commercial web site, such as e-bay.

Using Cal Poly email to apply for a grant.

- Using Cal Poly e-mail to communicate with potential employers.

A Cal Poly staff member uses the Cal Poly network to "telecommute" from home.

- An ASI student club uses its Cal Poly web page to announce an upcoming, approved event for which students will be charged a fee.
- The Cal Poly Animal Science Department uses their departmental web site to display photos of animals to be sold at an upcoming auction as part of an authorized enterprise project. Outside bidders are instructed to e-mail bids to the Cal Poly Foundation.
- A faculty member working as principal investigator on a University approved contract or grant asks departmental staff to convert digital data into the reporting format required by the funding agency.

Electronic Communications

- A student uses their Cal Poly e-mail account to send e-mail to friends and family.
- Incidental personal use by faculty and staff is reasonable provided it does not interfere with assigned work or negatively impact other users.
- With the approval of the department head and using a system alias, an administrative assistant e-mails every member of the department about an upcoming event.
- A faculty member e-mails an assignment to all the students in a course.
- A student, faculty or staff member deletes "spam" e-mail originating from a system other than Cal Poly or responds to the sender and asks to be removed.
- A faculty member creates a web page and includes a link to someone else's web page.
- Using Cal Poly e-mail to apply for an institutional grant.

Copyright

- A staff member is beta-testing software that can fix a problem on another staff member's machine. They contact the manufacturer and get permission to install the upgrade on the other person's machine which has a legally obtained copy of the current product installed.
- A student uses the same commands another person used to create a table on the web.
- A student posts photographs they took on their web page.
- A faculty member incorporates copyrighted materials in their course materials after first obtaining permission of the publishers of the materials.
- A faculty member distributes copies of a brief excerpt from a larger work in class and then retrieves the copies after class is over.

Information Technology Resources Responsible Use Policy (Interim)

Data Security

- A faculty member retrieves online information about a student in their class.
- A counselor reviews a student's record in order to counsel them as to which classes to take.
- A staff member uses SIS to generate a report about all the students in the department and their current status for the department head to review.

Harassment

- A student working on a computer in a lab creates or downloads one or more images that may disturb or offend others. They remove the images before leaving the facility or relocate to another workstation that is less visible to other users to work on this project.

Political Advocacy

- A faculty member uses University equipment to videotape or broadcast, with appropriate permissions, a live debate between candidates to students in a political science course.
- Posting an opinion about a candidate or issue to a newsgroup intended for that purpose.
- A student running for an ASI office uses a web page to discuss their platform and to collect e-mail addresses of potential supporters. The student uses the addresses to disseminate an e-mail message encouraging them to get students to vote in the election.
- A student uses a personal web page stored on Central UNIX to advocate on behalf of a particular candidate or ballot initiative.

Trademarks and Patents

- Displaying the Cal Poly logo on an "official" Cal Poly web page.

Inappropriate Uses

Authorized Use

- A student gives their login ID and password to a relative or friend outside of Cal Poly so they can post materials to the student's web site.
- A faculty member allows family members to use a Cal Poly account and Internet connection , to browse the web and to send e-mail from home.
- An administrator who is not using their Cal Poly account gives their login ID and password to the director of a local non-profit group who uses it to create a web page, send e-mail, etc.
- Without permission, a student accesses a faculty member's computer to view an insecure file containing test questions.

Information Technology Resources Responsible Use Policy (Interim)

Commercial Use

- Displaying personal items for sale on a web page residing on or transmitted through University resources.
- Displaying commercial advertisements on a web page hosted on University resources.
- Using a Cal Poly account to create and host a web site for a local organization promoting fundraisers and other commercial activities.
- Using a Cal Poly account to operate or conduct non-University related business activities, including financial management, advertising and promotion, correspondence, web sites, etc.
- An administrative assistant supplements income by typing senior projects and master thesis using a University workstation and laser printer in the office.
- A faculty member with an outside consulting business or working on a personal/individual government contract or grant not approved by the University makes extensive use of State resources frequently asks departmental staff to convert report documents into the format required by the agency and assist with various aspects of the project without compensating the departmentUniversity.
- Using the Cal Poly network to "telecommute" to non-University employers.

Electronic Communications

- A Cal Poly user forwards e-mail about a sick child and efforts to raise funds or send wishes or good luck to several other people on campus. The e-mail encourages recipients to pass the message along to as many people as possible.
- A Cal Poly user broadcasts a message on a current topic of interest to several newsgroups or system aliases, none of which have to do with that particular topic. For example, a user posts a message about abortion issues to a newsgroup about English poetry or sends a message about an upcoming student club event to a campus computing committee.

Copyright

- A department buys a single license copy of a software product and installs it on all the workstations in a student computer lab.
- Extensive excerpts from a copyrighted work are distributed by e-mail or displayed on a web page without obtaining the permission of the author/publisher.
- Photographs or images taken from another web page without the owner's permission are displayed on a web page residing on or accessed via University resources.
- In violation of the manufacturer's license agreement, a faculty or staff member installs software purchased for departmental use on their home computer or allows students to borrow software to install on their home machines.
- A student redistributes copies of software, music or other digital materials via the Internet. The student may have legally obtained these materials but does not have permission to redistribute them to others.

Information Technology Resources Responsible Use Policy (Interim)

- Using anonymous **FTP**, web sites, web servers, Napster or similar programs to provide access to illegally obtained or copyrighted materials used without proper permissions.

Data Security

- A faculty member is curious about the activities of a student and attempts to read any public access files in that student's central UNIX account.
- A student assistant with access to SIS uses that access to view other students' grades.
- A staff member discloses personal information to a relative of a student who has requested that their information not be disclosed.
- A staff member uses HRS to look up the home address and telephone number of a faculty member and gives that information to a student.
- A faculty member uses SIS to generate a mailing list of students in a specific discipline for the purpose of sending personal mail from home that is unrelated to University business.

Network/System Integrity

- Using Cal Poly resources, including the network, to propagate a computer virus, Trojan Horse, worm, and/or denial of service attack.
- A faculty member recklessly initiates a process on Central UNIX that causes response times to slow to a crawl and the system to be taken down and rebooted to fix the problem.
- Hosting an anonymous **FTP** server.
- Using any program that in anyway disrupts, harms, or infiltrates another computer, such as WinNuke, BackOrifice or a packet sniffer.
- Making extensive use of chat rooms and interactive games on the web, causing network and/or system performance to degrade.
- A dorm resident conducts a port scan of the residence hall network without permission of the network administrator.
- Anyone conducts any port scan of an external network via the Cal Poly network without permission of the network administrators.

Political Advocacy

- A student, staff or faculty member running for a local political office creates a web page to promote their candidacy, which resides on or is accessed via University resources.
- A faculty or staff member creates and uses an e-mail distribution list to solicit contributions, signatures, or other support on behalf of a particular candidate or ballot measure.

Information Technology Resources Responsible Use Policy (Interim)

Harassment

- Displaying an intimate, suggestive or disturbing image which a reasonable person would consider objectionable as the "wallpaper" or screen saver on a computer that is routinely visible to other students, staff and faculty.
- Repeatedly sending threatening or harassing e-mail or voice mail to another individual.

Trademarks and Patents

- Without obtaining permission in advance, a non-Cal Poly web site displays the Cal Poly logo, displays the Cal Poly home page design, or displays the University name in such a way as to imply University endorsement or affiliation.
- Without permission of the manufacturer, a user beta testing a new commercial software product loads it on a server and posts a message announcing that the software is available to anyone at that location.

Margaret R. Camuso

From: Mary K. Fiala
Sent: Monday, March 19, 2001 10:01 AM
to: Myron Hood
Cc: Dana L. Azevedo; Margaret R. Camuso; David Conn; Linda C. Dalton; Gladys E. Gregory; Joseph E. Grimes; Jerry J. Hanley; Kimi M. Ikeda; Bonnie T. Long; Valene B. Mathews; Kim Medina; Susan Mundahl; Paul J. Zingg
Subject: Response to AS-554-01 /IACC

On March 12, 2001, President Warren J. Baker responded, via memorandum, to Academic Senate Resolution AS-554-01/IACC-Resolution on Information Technology Resources Responsible Use Policy (RUP).

I have attached the President's response in its entirety as a Word document; however, I am also providing the text of the memorandum below for those who have e-mail systems that do not handle attachments.

If you have any questions, please call.

Mary K. Fiala
Executive Secretary to the President's Office
California Polytechnic State University
San Luis Obispo, CA 93407
805/756-6000 Fax: 805/756-1129
e-mail: mfiala@calpoly.edu

President Warren J. Baker's response of March 12, 2001, to Academic Senate Resolution AS-554-01/IACC-Resolution on Information Technology Resources Responsible Use Policy (RUP):

"I am pleased to approve Academic Senate Resolution AS-554-01/IACC-Resolution on Information Technology Resources Responsible Use Policy (RUP). By copy of this memorandum, I am asking that Jerry Hanley, Vice Provost/Chief Information Officer for Information Technology Services, implement the Responsible Use Policy, effective immediately.

In addition, in response to the Senate Resolution, I would also ask that any modifications and/or updates to the Responsible Use Policy be brought before the Instructional Advisory Committee on Computing (IACC) and be reported to the Academic Senate.

Please extend my appreciation to the IACC for its review of the RUP."