UC Merced Information Technology Resources
Acceptable Use Policy

(Approved 10/14/2003)

I. INTRODUCTION

The University fosters the use of information technology resources to store, process, and share information in support of the University's mission of teaching, research, and public service, and to conduct the University's business. To these ends, the University provides and supports facilities such as computers, networks, video and audio equipment, telecommunications devices, email, and the World Wide Web.

Incorporating the values affirmed by the UC Merced Principles of Community, this policy governs the use of information technology facilities at UC Merced. All UC Merced students, faculty, and staff, as well as others who may have been granted access to these resources, are responsible for adhering to this policy.

II. RIGHTS AND RESPONSIBILITIES

Information technology facilities provide access to resources on and off campus, as well as the ability to communicate with others worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all applicable laws, regulations, and contractual obligations. Because electronic information is generally easily reproduced and adaptable, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

The University is the legal owner and operator of all resources purchased or leased with University funds. Overall responsibility for administering the University's information technology resources is vested primarily in the Chief Information Officer (CIO). The CIO may delegate overall responsibility for certain resources.

Other organizations such as universities, companies, and governmental entities that operate resources that are accessible via the UC Merced network may have their own policies governing the use of those resources. When accessing remote resources from UC Merced facilities, users are responsible for following the policy of UC Merced and the remote facility, whichever is more restrictive.

III. PRIVACY

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of information technology resources. This policy reflects these principles within the context of the University's legal and other obligations. The University respects the privacy of electronic communications and stored information in the same way that it respects the privacy of paper correspondence and conversations, while seeking to ensure that University administrative records are accessible for the conduct of University business.

The University does not routinely inspect, monitor, or disclose electronic communications or stored information without the holder's consent. Nonetheless, the University may inspect, monitor, or disclose electronic communications and data files under certain limited circumstances, subject to the requirements for authorization, notification, and recourse under the guidelines of the UC Electronic Communications Policy and applicable UC Merced policies and procedures, except when these requirements are superseded by legal obligations.

IV. ENFORCEMENT OF LAWS AND UNIVERSITY POLICIES

Federal and state laws and University policies in some cases apply specifically to the use of information technology resources. In other cases they may apply generally to personal conduct in which the use of information technology resources is incidental.

Minor or accidental violations of the University of California Electronic Communications Policy, the UC Merced Acceptable Use Policy, or other related policies may be resolved informally by the department or unit administering the facilities involved. More serious violations (including repeated minor violations) may result in the temporary or permanent loss of access privileges or the modification of those privileges. Violators may be subject to disciplinary action up to and including dismissal or expulsion under applicable University

policies and collective bargaining agreements. Violators may be referred to their sponsoring advisor, supervisor, manager, dean, vice chancellor, Student Affairs representative, or other appropriate authority for further action.

V. UNACCEPTABLE CONDUCT

Conduct deemed unacceptable includes, but is not limited to, violation or attempted violation of the following principles:

A. Copyrights and licenses. Users shall respect copyrights and licensing agreements.
   1. Copying. Software shall not be copied except as permitted by copyright law or a license agreement.
   2. Number of simultaneous users. The number and distribution of copies shall be handled in such a way that the number of simultaneous users in a department does not exceed the number of licenses purchased by that department, unless otherwise stipulated in the purchase contract.
   3. Plagiarism. Copied material shall be properly attributed. Plagiarism of information in an electronic form is subject to the same sanctions as in any other medium.

B. Integrity of information technology resources. Users shall not interfere with the normal operation of information technology resources.
   1. Modification, damage, or removal. Users shall not modify, damage, or remove information technology resources that are owned by the University or other users without proper authorization.
   2. Encroaching on others' access and use. Users shall not encroach on others' access and use of the University's information technology resources. This includes but is not limited to: the sending of chain-letters or excessive messages; printing excessive copies; excessive use of network capacity; unauthorized modification of data, programs, and configurations; attempting to crash or tie up information technology facilities.
   3. Unauthorized or destructive programs. Users shall not intentionally develop or use programs such as, but not limited to viruses, backdoors, logic bombs, Trojan horses, bacteria, and worms that
      i. disrupt other users;
      ii. access private or restricted portions of the system;
      iii. identify security vulnerabilities or decrypt secure data, or
      iv. damage the software or hardware components of an electronic communications resource.

      Notwithstanding the above, the University recognizes the value of research and education in game development, computer security, the investigation of self-replicating code, and other similar pursuits. Such legitimate academic pursuits for research and instruction that are conducted under the supervision of academic personnel are authorized to the extent that the pursuits do not compromise the University's information technology facilities.
   4. Protecting network integrity. Users must ensure that proper security is implemented on computers for which they are responsible and that are connected to the network in order to protect the University against i) attempts to inappropriately access licensed and/or internal data and resources, or ii)“hacking” activities,. This includes performing reasonable and customary configuration and maintenance (including security updates, patches, etc.), as well as implementing and utilizing adequate access controls (proper passwords, secure protocols, etc.).
   5. Unauthorized equipment. Users shall not install or attach any equipment to the UC Merced network without the explicit approval of the Central Information Technology department or a designated delegate.

C. Unauthorized access. Users shall not seek or enable unauthorized access.
   1. Authorization. Users shall not access information technology resources without proper authorization, or intentionally enable others to do so.
   2. Password protection. A user who has been authorized to use a password-protected account shall not disclose the password or otherwise make the account available to others without authorization.

D. Usage. Users shall comply with applicable law and University policy.
   1. Hostile working environment or learning environment. Users shall not use information technology resources in a manner that creates a hostile working environment or learning environment (including sexual or other forms of harassment), or that violates obscenity laws.

2. Unlawful activities. Users shall not use information technology resources for unlawful activities or activities that violate University policy, including fraudulent, libelous, slanderous, harassing, threatening, or other communications,
3. Mass messaging. Users shall not spam, or otherwise transmit inappropriate mass messages to newsgroups, bulletin boards, mailing lists, or individuals. Postings to electronic mailing lists, bulletin boards, and similar facilities must be consistent with the stated purpose of the facility.
4. Information belonging to others. Users shall not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users.
5. False identity. Users shall not use the identity of another user without the explicit approval of that user, or mask the identity of an account or computer.
6. Implying University endorsement. Users shall not imply University endorsement of products or services of a non-University entity without explicit approval. This includes use of University information technology resources to convey such an endorsement.. Users shall not give the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the University unless authorized to do so. To avoid this, the user may use a disclaimer such as "The opinions or statements expressed herein are those of the author and do not represent the position of the University of California."

E. Personal, political, religious, and commercial use. The University is a not-for-profit, tax-exempt organization and, as such, is subject to applicable federal and state, laws and regulations on the use of University property. University users may use information technology resources for incidental personal purposes provided that such use does not: (a) directly or indirectly interfere with the University's operation of information technology resources, (b) interfere with the user's employment or other obligations to the University, (c) burden the University with noticeable incremental costs, or (d) violate the law or University policy. The following are examples of use which are restricted in this context.
1. Political use. The University of California Policy on Government Relations with State and Federal Officials governs the representation of the University in all matters requiring action by federal or state officials. The President of the University and his designees are authorized to represent the University on matters of budget and legislation at the state and federal level. While University constituents (faculty, students, administrators, staff and volunteers) are free to exercise their First Amendment rights to communicate with elected officials on public issues of personal interest, letters to elected officials or their staff from faculty, staff, administrators, or students expressing personal views may not be written on University letterhead nor sent in an email from a University computer or electronic email address. Faculty members are encouraged to share their subject matter expertise with elected officials and their staff, in line with the University public service mission, but must avoid seeking state or federal legislative or budget support for their projects and must state that their verbal or written comments (including those transmitted through electronic mail) do not represent an official position of the University of California. The UC Merced Director of Government Relations will provide guidance and assistance to faculty who are providing subject matter expertise to elected officials or their staff on issues where they are not officially representing the University. Questions related to expression of political views by faculty, staff, or students as individuals through University information technology resources should be directed to the UC Merced Director of Government Relations.
2. Religious use. In incidental communications relating to religious activities or issues, the user's University title and/or affiliation may be used only for purposes of identification. A disclaimer (see D.6 above) must be used if such identification might reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any religious activity or issue.
3. Commercial use. University information technology resources shall not be used for non-University commercial purposes, except as permitted under University policy or with the appropriate approval.
4. Advertisements. The University's information technology facilities shall not be used to transmit commercial or personal advertisements, solicitations, or promotions, except as permitted under University policy or with the appropriate approval.