Acceptable Use Policy

I. Introduction

The University encourages the use of electronic communications to share information and knowledge in support of the University's mission of education, research, community service, and patient care, and to conduct the University's business. To these ends, the University supports and provides electronic communications resources such as computers, networks, video and audio equipment, telecommunications devices, email, and the World Wide Web.

Incorporating the values affirmed by the UC Davis Principles of Community, this policy governs the use of electronic communications resources at UC Davis. All UC Davis users are responsible for reading and understanding this policy. Users must acknowledge, in writing, that they have read and understand this policy before they are allowed access to UC Davis electronic communications resources.

II. Rights and Responsibilities

Electronic communications provide access to resources on and off campus, as well as the ability to communicate with other users 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 relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, 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 electronic communications resources purchased or leased with University funds. Overall responsibility for administering the University's electronic communications resources is primarily that of the Vice Provost--Information & Educational Technology. The Vice Provost--Information & Educational Technology may delegate overall responsibility for certain resources.

Other organizations such as universities, companies, and governments that operate resources that are accessible via the UC Davis network may have their own policies governing the use of those resources. When accessing remote resources from UC Davis facilities, users are responsible for following the policy of UC Davis and/or 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 electronic communications 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 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 without the holder's consent. Nonetheless, the University may deny access to its electronic communications resources and may inspect, monitor, or disclose electronic communications under certain limited circumstances, subject to the requirements for authorization, notification, and recourse in the UC and UC Davis Electronic Communications Policies.

IV.   **Enforcement of Laws and University Policies**

Federal and state laws and University policies apply to electronic communications resources, including not only those that are specific to computers, but also those that apply generally to personal conduct.

Minor or accidental violations of this policy may be handled informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussion and education.

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 Judicial Affairs, or the Misuse of University Resources Coordinating Committee or other appropriate authority for further action.

V.   **Unacceptable Conduct**

Unacceptable conduct includes, but is not limited to, the following attempted or completed actions:

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 copies purchased by that department, unless otherwise stipulated in the purchase contract.

   3.   Plagiarism. Copied material shall be properly attributed. Plagiarism of electronic communications information is subject to the same sanctions as in any other medium.

B.   Integrity of electronic communications resources. Users shall not interfere with the normal operation of electronic communications resources.

   1.   Modification, damage, or removal. Users shall not modify, damage, or remove electronic communications 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 electronic communications resources. This includes but is not limited to: the sending of chain-letters or excessive messages; printing excessive copies; running grossly inefficient programs when efficient alternatives are available; unauthorized modification of electronic communications resources; attempting to crash or tie up electronic communications resources.

   3.   Unauthorized or destructive programs. Users shall not intentionally develop or use programs such as, but not limited to, viruses, backdoors, and worms that disrupt other

users, access private or restricted portions of the system, identify security vulnerabilities, decrypt secure data, or damage the software or hardware components of an electronic communications resource. Legitimate academic pursuits for research and instruction that are conducted under the supervision of academic personnel are authorized by the Vice Provost—Information and Educational Technology to the extent that the pursuits do not compromise the University's electronic communications resources.

4.   Unauthorized equipment. Users shall not install or attach any equipment to a UCD electronic communications resource without the explicit approval of the system administrator for that electronic communications resource.

C.   Unauthorized access. Users shall not seek or enable unauthorized access.

1.   Authorization. Users shall not access electronic communications 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.

3.   Misuse of EC records. Users may seek out, use, or disclose information contained in EC records only for University business.

D.   Usage. Users shall comply with applicable law and University policy.

1.   Hostile working environment. Users shall not use electronic communications resources in a manner that creates a hostile working environment (including sexual or other forms of harassment), or that violates obscenity laws.

2.   Unlawful activities. Users shall not use electronic communications resources for unlawful activities or activities that violate University policy, including fraudulent, libelous, slanderous, harassing, threatening, or other communications.

3.   Mass messaging. Users shall avoid spamming, and other inappropriate mass messaging to newsgroups, bulletin boards, mailing lists, or individuals. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list so long as the material is consistent with the list's purpose.

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 machine.

6.   Implying University endorsement. Users shall not imply University endorsement of products or services of a non-University entity from a University electronic communications resource without approval. 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 should not be taken as a position of or endorsement by the University of California."

7.   Protection of restricted personal information. Employees are responsible for maintaining the security of individual's restricted personal information. Restricted personal information that is not necessary for an employees position responsibilities shall be removed from electronic communication devices. If the security of restricted personal information is compromised (e.g., loss of computer, theft, hacking), the employee must immediately inform their supervisor and the Security Coordinator at security@ucdavis.edu.

E.   Political, religious, personal, and commercial use. The University is a not-for-profit, tax-exempt organization and, as such, is subject to federal, state, and local laws on the use of University property.

1.   Political or religious use. In communications relating to religious or political activities or issues, the user's University title may be used only for identification. If such identification might reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any religious or political activity or issue, a disclaimer (see D.6 above) shall be used.

2.   Personal use. University users may use electronic communications resources for incidental personal purposes provided that such use does not: (a) directly or indirectly interfere with the University's operation of electronic communications 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.

3.   Commercial use. University electronic communications 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 electronic communications resources shall not be used to transmit commercial or personal advertisements, solicitations, or promotions, except as permitted under University policy or with the appropriate approval.

VI.   Further Information

UC Davis Policy & Procedure Manual Sections 310-23 and 310-24 (available on the Web at http://manuals.ucdavis.edu), and the University of California Electronic Communications Policy (available on the Web at http://www.ucop.edu/ucophome/policies/ec/), give further information and a list of relevant federal and state laws and University policies.

The Information & Educational Technology Services Website at http://iet.ucdavis.edu/ provides information on the use of the University's electronic communications resources.