UNIVERSITY MANAGEMENT LETTER 01-02

Guidelines for Responsible Computing at Humboldt State University

(Appropriate Use Policy)

April 2001

(Supersedes UML 96-8)

This document borrows extensively from and replicates significant portions of the University of Delaware's "Policy for Responsible Computing." The University of Delaware was awarded CAUSE's "Best Practices in Service" award for 1995 for this work. Local modifications and editing were performed by a committee of users in 1996, including faculty, staff, and students, appointed by the Vice President for Academic Affairs. Some wording in the document was updated in 2001 to bring the wording into conformance with the California State University 4CNet Appropriate Use Policy (2000) and its Recommended Contextual Standards for Appropriate Use Policies (2000).

Preface

It is imperative that all users of the University's computing, communications, and information resources realize how much these resources require responsible behavior from all users. Simply put, we are all responsible for the well-being of the computing, network, and information resources we use.

Universities do try to promote the open exchange of ideas; however, an open, cooperative computing network can be vulnerable to abuse or misuse. As more and more schools, colleges, universities, businesses, government agencies, and other enterprises become attached to the world-wide computing and information networks, it is more important than ever that this University educate its students, faculty, and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues. A modern university must also educate its students, faculty, and staff about how computer abuse can interfere with the exchange of ideas that is integral to a modern education.

The first item in the body of this document is the Humboldt State University Appropriate Use Policy. The remainder of this document consists of guidelines for implementing this policy.

If you have any questions about the policy or the guidelines, please consult with your system administrator; the Help Desk or other staff in Information Technology Services; or with your dean, project director, supervisor, chair, or advisor; or the Information Security Coordinator.

Humboldt State University Appropriate Use Policy

In support of its mission of teaching, research, and public service, Humboldt State University provides access to computing, communications, and information resources for students, faculty, and staff within institutional priorities and financial capabilities.

The Humboldt State University Appropriate Use Policy contains the governing philosophy for regulating faculty, student, and staff use of the University's computing, communications, and information resources. It spells out the general principles regarding appropriate use of data, equipment, software, and networks. By adopting this policy, the Executive Committee recognizes that all members of the University are also bound by local, state, and federal laws and other statutes relating to copyrights, security, electronic media and intellectual property.

☞ **Policy**

All users of the University's computing, communications, and information resources must act responsibly. Every user is responsible for the integrity of these resources. All users of University-owned or University-leased computing and communications systems, whether managed directly or indirectly by the campus, must respect the rights of other computing and communications users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements. It is the policy of Humboldt State University that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the relevant faculty, staff and student standard of ethics and conduct. Additionally, all users must comply with the California State University 4CNet Appropriate Use Policy.

The University reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Access to the University's computing and communications facilities is a privilege granted to University students, faculty, and staff. Access to University information resources may be granted by the data owners based on the data owner's judgment, which would include the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the University.

Data owners--whether departments, units, faculty, students, or staff--may allow individuals other than University faculty, staff, and students access to information for which they are responsible through methods approved by and at the discretion of the system administrator, so long as such access does not violate any license or contractual agreement; University policy; or any federal, state, county, or local law or ordinance; or degrade the performance of the University's information service to the detriment of the University community.

University computing and communications facilities and accounts are to be used for the University-related activities for which they are assigned. All computing and network resources are provided only to support the academic mission of the University. University computing and communications resources are not to be used for commercial purposes or non-University-related activities without written authorization from the University. If the University grants such authorization, the University may assess appropriate charges to recover the costs of providing such services. This policy applies equally to all University-owned or University-leased computers and network resources.

Abuse of computing and/or communications privileges is subject to disciplinary action as well as loss of computing and communications privileges and/or the assessment of fines to recover any costs for investigations and the value of resources used. Abuse of the University's computing and communications resources may also result in loss of university privileges, dismissal, or civil/criminal action. Nothing in these guidelines precludes enforcement under the laws and regulations of the State of California, any municipality or county therein, and/or the United States of America. For example, if a user is found guilty of committing a computer crime as outlined in the California Penal Code 502, *Computer Crimes*, and 502.1, *Computer crime penalty, forfeiture of property*, he or she could be subject to the penalties for a felony.

The use of electronic communications in violation of University policies on affirmative action and nondiscrimination is subject to disciplinary action under those policies and also violates this Appropriate Use Policy. University policy statements on affirmative action and nondiscrimination (including harassment) are available in the Office of Institutional Equity, Affirmative Action, and Diversity. Disciplinary actions pursuant to violations of the Appropriate Use Policy are defined herein.

☞ **Implementation**

Appropriate University administrative officers should adopt guidelines for the implementation of this policy within each unit and regularly revise these guidelines as circumstances, including but not limited to changes in technology, warrant. Copies of these guidelines should be forwarded to the Director of Information Technology Services. The Director of Information Technology Services shall, from time to time, recommend adjustments to the guidelines to assist departments and units with this effort.

As an aid to a better understanding of responsible computing practices, all departments that own or lease computing equipment are encouraged to develop "Conditions Of Use" documentation for all systems that they operate and to make these documents available to users. These documents must be consistent with the "Humboldt State University Appropriate Use Policy" and should be approved by the department's administrative officer or other individual designated by that administrative officer.

☞ **Enforcement**

Users and system administrators must all guard against abuses that disrupt or threaten the viability of all systems, including those at the University and those on networks to which the University's systems are connected. Access to information resources without proper authorization from the data owner, unauthorized use of University computing or communications facilities, or intentional corruption or misuse of information resources is forbidden, and may subject the violator to sanctions available under this and/or other University policies and/or civil and/or criminal liability under the California Penal Code 502 *Computer Crimes* and 502.01 *Computer crime penalty; forfeiture of property.*

User Responsibilities

If you use the University's computing resources or facilities, you have the following responsibilities:

- Use the University's computing facilities and information resources, including hardware, software, networks, and computer accounts, (in accordance with these guidelines) respecting the rights of other computing users and respecting all contractual and license agreements. University facilities are not available for commercial use or profit unless specific contractual agreements have been made.

- Use only those computers and computer accounts for which you have authorization.

- Use mainframe accounts only for the purpose(s) for which they have been issued. Use University-owned microcomputers and advanced workstations for University-related projects only.

- Be responsible for all use of your accounts and for protecting each account's password. In other words, do not share computer accounts. If someone else learns your password, you must change it.

- Report unauthorized use of your accounts to your project director, instructor, supervisor, system administrator, or other appropriate University authority immediately upon discovery.

- Cooperate with system administrator requests for information about computing activities. During an investigation (formal or informal), a system administrator is authorized to inspect your computer files. Note that users of the University's information technology resources have no inherent right to privacy for the content of information they store on University-owned or leased computing resources or transmittal over University-owned or leased networks, and system administrators may have to examine that content as part of an investigation. Further, supervisors have the right to inspect the contents of files created on University-owned or leased computers by employees reporting to them.

- Take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully fulfilled on any system, network, or server that you operate.

- Each user is ultimately responsible for his or her own computing and his or her own work using a computer. Take this responsibility seriously. For example, users should remember to make backup copies of their data, files, programs, diskettes, and tapes, particularly those created on microcomputers and those used on individually or departmentally operated systems. Furthermore, users with desktop computers or other computers that they operate themselves must protect the integrity of those systems as if they were the system administrators for those computers and need to take that responsibility very seriously.

- If you are a project director for a group of mainframe computing users, a supervisor whose staff uses computers, or a faculty member whose students use computers, you must ensure your project members, staff, or students are informed about the Guidelines for Responsible Computing at Humboldt State University.

System Administrator Responsibilities

A system administrator's use of the University's computing resources is governed by the same guidelines as any other user's computing activity. However, a system administrator has additional responsibilities to the users of the network, site, system, or systems he or she administers:

- A system administrator manages systems, networks, and servers to provide available software and hardware to users for their University computing. A "system" includes user desktop, portable, and other computers for which the system administrator has been assigned support responsibility.

- A system administrator is responsible for the security of a system, network, or server.

- A system administrator shall take reasonable and appropriate steps to see that all the terms of the hardware and software license agreements are faithfully fulfilled on all systems, networks, and servers for which he or she has responsibility.

- A system administrator shall take reasonable precautions to guard against corruption of data or software or damage to hardware or facilities.

- A system administrator's access to a user's information shall be governed by relevant state and federal privacy law.

If a system administrator:

- is an eyewitness to a computing abuse,
- notices an unusual degradation of service or other aberrant behavior on the system, network, or server for which he or she is responsible,
- receives a complaint or report of suspected computing abuse or degradation of service, or
- is alerted by system-monitoring or management software that indicates a potential security intrusion,

then he or she should investigate and take steps to protect the integrity of the system entrusted to his or her care, including, if necessary, disabling a system or user account which may be the source of the aberrant behavior or potential security intrusion; respect the confidentiality of the information users have stored on the system; notify his or her administrative officer if the above two aims come into conflict; and assist his or her administrative officer in referring cases of suspected abuse to the appropriate University judicial process.

Misuse of Computing, Communications, and Information Resource Privileges

The University characterizes misuse of computing, communications, and information resource privileges as improper and as just cause for taking disciplinary action and/or revoking computer privileges. Misuse of computing, communications, and information resource privileges includes, but is not restricted to, the following:

- Attempting to modify or remove computer equipment, software, or peripherals without proper authorization from the systems administrator.
- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the University (i.e., if you abuse the networks to which the University belongs or the computers at other sites connected to those networks, the University will treat this matter as an abuse of your Humboldt State University computing and communications privileges).
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security processes.
- Using computing facilities, computer accounts, or computer data for purposes other than those for which they were intended or authorized.
- Sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading someone else's electronic mail without his or her permission.

- Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, and fraudulent electronic authorization of purchase requisitions or journal vouchers.

- Violating any software license agreement or copyright, including installing, copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

- Violating the property rights of copyright holders who are in possession of computer-generated data, reports, or software.

- Using the University's computing resources to harass or threaten other users. Harassment includes, but is not limited to, any behavior that

    1. involves an expressed or implied threat to an individual's academic efforts, employment, participation in University-sponsored extracurricular activities or personal safety; OR
    2. has the purpose or reasonably foreseeable effect of interfering with an individual's academic efforts, employment, participation in University-sponsored extracurricular activities or personal safety; OR
    3. creates an intimidating, hostile or demeaning environment for educational pursuits, employment or participation in University-sponsored extracurricular activities.

- Displaying on screens in shared facilities images, sounds, or messages which could create an atmosphere of discomfort or harassment to others. Students should make arrangements through their instructor for a private work area if a class assignment requires them to access such materials.

- Taking advantage of another user's naivete or oversights to gain access to any computer account, data, software, or file that is not your own and for which you have not received explicit authorization to access.

- Physically interfering with other users' access to the University's computing facilities.

- Encroaching on others' use of the University's computers (e.g., disrupting others' computer use by excessive game playing; by sending excessive messages, either locally or off-campus, including but not limited to electronic chain letters; printing excessive copies of documents, files, data, or programs).

- Modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer; damaging or vandalizing University computing facilities, equipment, software, or computer files.

- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner except when so authorized as a system administrator or performing the duties of supervisor.

- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission except when so authorized as a system administrator or performing the duties of supervisor.

- Using university facilities for commercial use or profit unless specific contractual agreements have been made.

Administrative Process for Cases of Misuse of Computing, Communications, or Information Resource Privileges

If staff in the University Police Department/Public Safety or system administrators have information that misuse of computing resources has occurred, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

- Take action to protect the system(s), user jobs, and user files from damage.

- Notify the alleged abuser's project director, instructor, academic advisor, dean, or administrative officer of the investigation.

- Refer the matter for processing through the appropriate University administrative process. If necessary, staff members from a central computing agency such as Information Technology Services as well as faculty members with computing expertise may be called upon to advise the University judicial officers on the implications of the evidence presented and, in the event of a finding of guilt, of the seriousness of the offense.

- Suspend or restrict the alleged abuser's computing privileges during the investigation and administrative processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the University's administrative process, through the grievance procedures outlined in University collective bargaining agreements, or by petition to the Vice President of Student Affairs, as appropriate.

- Inspect the alleged abuser's files, diskettes, and/or tapes. System administrators shall have a trail of evidence that leads to the user's computing activities or computing files before inspecting any user's files.

Ordinarily, the administrative officer whose department is responsible for the computing system on which the alleged misuse occurred should initiate the administrative proceedings. As the case develops, other administrative officers may, by mutual agreement, assume part of the responsibility for prosecuting the case.

Academic Honesty

Students are reminded that computer-assisted plagiarism is still plagiarism. Unless specifically authorized by a class instructor, all of the following uses of a computer are violations of the University's guidelines for academic honesty and are punishable as acts of plagiarism:

- copying a computer file that contains another student's assignment and submitting it as your own work.
- copying a computer file that contains another student's assignment and using it as a model for your own assignment.
- working together on an assignment, sharing the computer files or programs involved, and then submitting individual copies of the assignment as your own individual work.
- knowingly allowing another student to copy or use one of your computer files and to submit that file, or a modification thereof, as his or her individual work.

For further information on this topic, students are urged to consult the "Fine Print" section of the Humboldt State University Catalog and/or to consult with their individual instructors.

All users are urged to consult the Humboldt State University Intellectual Property Policy (available from the Office for the Dean for Research and Graduate Studies). Faculty also should consult the relevant provisions of the Collective Bargaining Agreement.

Disclaimer

The software made available by the University has been licensed by the University for your use. As a result, its use may be subject to certain limitations.

The University is not responsible for loss of information from computing misuse, malfunction of computing hardware, malfunction of computing software, or external contamination of data or programs. The staff in central computing units such as Information Technology Services and all other system administrators must make every effort to ensure the integrity of the University's computer systems and the information stored thereon. However, users must be aware that no security or back-up system is 100.00% foolproof.

Definition of Terms

Administrative Officer:

employee of the University with supervisory responsibility over a unit of the University which operates Information Resources.

Computer Account:
: the combination of a user number, username, or userid and a password that allows an individual access to a mainframe computer or some other shared computer or network.

Data Owner:
: the individual or department that can authorize access to information, data, or software and that is responsible for the integrity and accuracy of that information, data, or software. The data owner can be the author of the information, data, or software or can be the individual or department that has negotiated a license for the University's use of the information, data, or software.

Desktop Computers, Microcomputers, Advanced Workstations:
: different classes of smaller computers, some shared, some single-user systems. If owned or leased by the University or if owned by an individual and connected to a University-owned, leased, or operated network, use of these computers is covered by the Appropriate Use Policy.

Executive Committee:
: consists of the President, Executive Assistant to the President and the Vice Presidents.

Information Resources:
: in the context of these Guidelines, this phrase refers to data or information and the software and hardware that makes that data or information available to users.

Mainframe Computers:
: "central" computers capable of use by several people at once. Also referred to as "time-sharing systems."

Network:
: a group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

Normal Resource Limits:
: the amount of disk space, memory, printing, etc., allocated to your computer account by that computer's system administrator.

Peripherals:
: special-purpose devices attached to a computer or computer network--for example, printers, scanners, plotters, etc.

Project Director:
: person charged with administering a group of computer accounts and the computing resources used by the people using those computer accounts.

Server:
: a computer that contains information shared by other computers on a network.

Software:
: programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.). Usually used to refer to computer programs.

System Administrator:
: staff employed by a central computing agency such as Information Technology Services whose responsibilities include system, site, or network administration and staff employed by other University departments whose duties include system, site, or network administration. System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. If you have a computer

on your desk, you may be acting, in whole or in part, as that computer's system administrator.

User:

someone who does not have system administrator responsibilities for a computer system or network but who makes use of that computer system or network. A user is still responsible for his or her use of the computer and for learning proper data management strategies.

Humboldt State University Home Page URL of this document:
http://www.humboldt.edu/~its/planning/policy/aup.html

Approved: September 19, 1996
Revised: March 16, 2001
Revision approved: April 5, 2001

Please refer comments and questions regarding this document to the Information Security Coordinator at security@humboldt.edu.

Distribution: Deans, Directors, Department Chairs