UO Acceptable Use of Computing Resources Policy

This document presents policies for acceptable use of University of Oregon computing resources. It neither reduces nor expands existing acceptable-use policies, but merely clarifies and illustrates the sorts of behaviors that may result in a response by the university or other interested parties. If you have questions about the acceptability of a particular use of computing resources, contact the Chief Information Security Officer (ciso@uoregon.edu) to assist you in clarifying the issues involved. While staff members do not provide legal advice, they can help you review technical issues and explain what is generally considered to be acceptable or unacceptable behavior.

An addendum to this document, “Amendments to State of Oregon Policies on Acceptable Use of State Electronic Information Systems,” outlines the university's departures from statewide acceptable use regulations. View the Acceptable Use Policy Addendum.

Appropriate Use of Computing Resources

When you are provided access to university computing resources, your use of them may be explicitly or implicitly limited. For example, if you are given access to an administrative computing system solely to enter accounting information or prepare class rosters, it is inappropriate for you to use the system to play a compute-intensive online computer game. Access to administrative systems should be used solely for the purposes for which the access was provided.

The situation with academic timesharing computers and microcomputer labs is less narrowly defined. As with the university library, access to academic computing resources is provided in part so you can learn, explore, and grow as part of your education or employment at the university. However, activities related to the university's scholarly mission take precedence over computing pursuits of a more personal or recreational nature. For example, those completing class assignments or conducting research for a graduate program or publication have priority over those using computing resources to process personal email, explore network resources, etc.

Some applications (such as Muds/Moos/Mucks/Mushes, IRC, Talk, and online computer games) may be unsupported or actively discouraged, due to the demands they place on our limited modem pool, CPU, and lab resources. Please cooperate with Computing Center staff if you are asked to refrain from running applications like these when resource use is heavy.

Prohibited Conduct

The University Conduct Code, OAR 571-21-030, also applies to electronic forums. The code prohibits, among other things, lewd or indecent conduct, threat of imminent physical harm, sexual or other harassment, stalking, forgery, intentional disruption of university services, and damaging or destroying university property. Similarly, the code's prohibitions against illegal

discrimination, including discriminatory harassment and sexual harassment, also apply to electronic forums.

Sharing of Accounts or Lab Passes Prohibited

As a result of enrolling or being employed by the university, certain computing resources may be made available for your use. The university manages access to its limited computing resources by requiring that users identify their accounts with a unique personal user name and a secret password, or present a lab pass or sticker they obtained. Sharing an account or lab pass with others is prohibited; i.e., authorization to use university computing resources is not shareable or transferable.

Information Services staff members are pleased to assist you in getting properly authorized to access the resources you need. We are also prepared to discuss alternative service providers with you if you are not eligible to access computing resources at the university.

Unauthorized use or misuse of university computing resources may constitute theft of services, and may be criminally punishable. Violators may also be civilly liable for the value of the stolen resources.

Commercial Use of Resources Prohibited

The university is committed to ensuring that all commercial enterprises have equal opportunity to conduct business. This might not be possible if the university unwittingly underwrote some enterprises by providing access to computing resources which could then be commercially exploited. Moreover, in many instances the university negotiates special academic pricing agreements for obtaining the computing resources it needs. Most such agreements are contingent upon the university prohibiting commercial use of the resources. Breaching educational licensing agreements could have serious financial consequences for the UO. Thus, commercial use of the university's computing resources is strictly prohibited.

Note: While chain letters may or may not be considered a commercial use of computing resources per se, you may not use university computing resources to transmit or propagate chain letters.

Violations of Electronic Privacy

Access to electronic files, network communications, email, voicemail, and any other related data is protected by various Federal statutes, including the Electronic Communication Privacy Act. Like an unauthorized telephone wiretap, unauthorized access to a person’s electronic data is prohibited, and may subject the perpetrator to serious penalties. Examples of specifically prohibited behaviors include:

- unauthorized interception or diversion of network transmissions
- accessing clearly confidential files that may be inadvertently publicly readable

- accessing confidential information about a person (such as their educational records) without their consent or other authorization

Keep in mind that shared systems are inherently insecure. Authorized Information Services or computer lab staff may access accounts and transmissions for troubleshooting and maintenance--and, if there is reasonable suspicion of misuse, they may access them for investigative purposes. You should also be aware that security systems whose purpose is to identify unauthorized users of a system may also monitor authorized users.

In general, material whose privacy must be guaranteed should not be stored on shared computers. Good quality encryption tools are now widely available, and should be used whenever you work with sensitive information.

Interference with Computer Use or Operations

Efforts to interfere with the use or operation of computing or networking resources are prohibited. These include:

- unauthorized use of these resources
- distribution of computer viruses, worms, trojan horse programs, email “bombs,” chain letters, etc.
- actions that result in the denial of service to other users by triggering system security features, or intentionally misconfiguring equipment to render it unusable
- forged or counterfeited email messages
- posting USENET News articles to inappropriate newsgroups, posting to moderated newsgroups without the approval of the moderator, or cross-posting articles to many newsgroups simultaneously (“spamming”)
- interference with the use of microcomputers, X terminals, or other workstations by the unauthorized display of output on such devices without the assent of the individual currently using the device

We ask that you cooperate with system administrators if you are advised of potential security problems associated with your account or system.

Recognition of Copyrights

The University of Oregon respects copyright laws and insists that its faculty, students, and staff do likewise. Copying proprietary software is theft, and will not be tolerated on campus. Illegally copied software subjects the university to risk of litigation, and denies software authors the compensation they deserve. Moreover, use of such software could result in your suspension or dismissal from the university, and either criminal prosecution or a civil suit for copyright infringement, or both.

Similarly, if you make materials available for others to retrieve or use (via a World Wide Web server, postings to a USENET newsgroup, etc.), be sure to respect their copyrights. In general,

every document, image, or sound is copywritten upon creation, and may only be used or redistributed with the permission of the copyright holder.

Wise Use of Limited Resources

Given the university's limited resources, as well as the direct social costs accrued from wasteful behavior (such as printing output that isn't needed), we ask that you be careful how you use computing resources, especially

- tangible resources (such as printing) where excessive use translates into additional real costs
- shared finite resources (e.g., timesharing CPU cycles, dial-in modem time, disk space, or Internet bandwidth), where selfish behavior on the part of a few can prevent many others from doing their work

Please cooperate in helping us make the most of the limited resources we have available.

Personal Responsibility for Online Statements

We all enjoy our constitutionally protected right to free speech and the tradition of academic freedom here at the UO. However, with these freedoms comes responsibility for what you say and write. If you defame someone online or invade his or her privacy, you may be sued. Exercise your freedom to speak out, but do so responsibly and in a way that reflects creditably on the university.

Disciplinary Action

Violations of these policies that constitute a breach of the Student Conduct Code or the Faculty Handbook will be referred to appropriate authorities. Information Services personnel may take immediate action, as needed, to abate ongoing interference with network and system operations, or to ensure system integrity.

If you have questions related to acceptable use of UO computing services, please contact the Chief Information Security Officer (ciso@uoregon.edu).