Acceptable Use of Computing Resources

Addendum: Amendments to State of Oregon Policies on Acceptable Use of State Electronic Information Systems (Version 3: 8/1/97)

1. Introduction

This document has been prepared pursuant to DAS 03-21 "Acceptable Use of State Electronic Information Systems," dated 2/20/97, which provides general State of Oregon policy on acceptable use of state electronic information systems (see attached copy of DAS 03-21 policies and standards). DAS 03-21 specifically recognizes that "The agency may adopt its written policy to replace or amend this broad, statewide policy to its specific needs." By this document, the University of Oregon is replacing/amending that policy to meet its specific needs within the context of its mission.

2. Relationship to the University's Existing "Acceptable Use of Computing Resources" Document

All terms and provisions of the UO's "Acceptable Use of Computing Resources" document are hereby incorporated by reference, and continue in full force and effect.

3. Organization of this Document

The sections of this document follow essentially the same order as the sections in DAS 03-21; we have annotated the section headings to facilitate cross-references between the two documents.

4. Ownership of Systems and Information [DAS 03-21: "Systems and Information are State Property"]

Ownership of electronic information systems, including physical systems, software, and information stored on those systems, is comparable to ownership of non-electronic University resources.

Tangible Assets. Thus, for example, tangible electronic information systems purchased with state funds are owned by the state, just as a vehicle or a laboratory instrument purchased with state funds is owned by the state.

Licensed Software. Software used on electronic information systems is customarily procured subject to licensing terms that may grant the state a non-exclusive, non-transferable and otherwise limited license, rather than absolute and unqualified ownership. In all cases, it is and shall be the University's policy and desire to scrupulously observe all copyrights and all contractual software licensing terms pertaining to software it purchases.

Information and Data. The state may or may not have a property interest in information stored on University systems. Mere physical presence of information on a University electronic information system is not sufficient to conclusively establish the ownership and control of that information, just as physical presence of a paper document in a faculty member's desk or filing cabinet does not establish an irrefutable presumption that the document is owned or controlled by the University.

At the same time, the University does clearly own, control, or have a custodial relationship with respect to certain classes of information stored on its electronic information systems, including, but not limited to

- administrative data (such as payroll and personnel data; student enrollment and grade information; accounting records, such as accounts receivable, accounts payable, and general ledger information; etc.)
- records required to be retained for archival purposes, including electronic messages pertaining to University planning, budgeting, operations, governance, and deliberative activities
- proprietary information produced as a work for hire or produced during the course of University-subsidized research or investigations, subject to the University's established policies for technology transfer and intellectual property rights

University Information or Data Not Stored on University Electronic Information Systems. Similarly, the University recognizes that information or data not stored on University electronic information systems may nonetheless belong to or be subject to the control of the University. For example, UO data or information might conceivably be stored on magnetic media at a national supercomputer center or on a commercial Internet service provider's equipment, just as University documents might be temporarily stored at a faculty member's home or at an alternate location while the faculty member is on sabbatical. Put simply, the physical location of data or information does not conclusively determine its ownership.

5. Appropriate Use of Electronic Information Systems [DAS 03-21: "Systems are for Agency Business"]

[the following section is taken from the University's "Acceptable Use…" document, version 1.6, June 1997]:

When you are provided access to University electronic information systems, 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 e-mail, 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 University Computing staff if you are asked to refrain from running applications like these when resource use is heavy.

6. Access and Control [DAS 03-21: "Agency has Full Access and Control"]

[the following section is adapted from the UO's "Acceptable Use…" document, version 1.6, June 1997]

Access to electronic files, network communications, and related data is protected by various Federal statutes, including in limited instances 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 or administrative deauthorizations. Examples of specifically prohibited behaviors include

- unauthorized interception or diversion of network transmissions
- accessing clearly confidential files that may be inadvertently publicly readable or the security for which a user has circumvented or overridden
- accessing confidential information about a person (such as their educational records) without their consent or authorization

Keep in mind that shared systems are inherently insecure. Authorized Computing Center or computer lab staff may access accounts and transmissions for troubleshooting and maintenances. And, if there is reasonable suspicion of misuse, or if such accounts, transmissions, and electronic files may contain evidence of prohibited, deliberatively deceptive, fraudulent, unauthorized, illegal, or criminal behavior, the staff 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 (such as PGP) are now widely available, and should be used whenever you work with information of a sensitive nature.

Cryptographic Security Systems. The University explicitly recognizes that routine operational data and system security requirements may necessitate the use of cryptographic security systems including, but not limited to, secret account passwords, file encryption, and encrypted data streams ("scrambled transmissions"). Use of such techniques is hereby explicitly authorized by the University in all cases, provided that the motive for using cryptographic security techniques is improved operational security for University business and/or compliance with federal or state requirements, and

- provided, in the case of secret account passwords, the password must be able to be reset by an authorized system administrator in the event the password is forgotten, the employee dies or is incapacitated, is unavailable due to travel, etc. As a matter of policy, passwords shall not be shared nor recorded in unencrypted form.
- provided, in the case of encrypted files, the person responsible for the encrypted data has explicitly considered the risk that the data might be irrecoverably lost in the event decryption cannot be performed for whatever reason, and, having considered that risk, believes the benefits of encryption substantially outweigh the risk of the file's contents being irrevocably lost.
- provided, in the case of scrambled transmissions, it is possible to ascertain a responsible party at the University of Oregon who is originating, receiving, or controlling the scrambled transmission, and who can answer inquiries concerning those transmissions, should questions about the transmissions arise.

Review/Screening of Information That Originates At, Is Intended For, or Happens to Incidentally Transit University Systems. DAS 03-21 provides notice that "The agency intends to...review, audit,...block, restrict, screen,... any information [from a state electronic information system], at any time without notice."

It is the University's opinion that it is not currently technically possible, nor necessarily desirable or advisable, for the University to review, audit, block, restrict or screen all the information that originates at, is intended for, or happens to incidentally transit its electronic information systems.

The University will, however, be responsive to reports it may receive about inappropriate use of electronic information systems. The University also reserves the right to employ screening mechanisms to filter unsolicited commercial e-mail ("UCE" or "spam") or other materials that the University determines to be meritless, commercially exploitive of state resources, or otherwise violative of our acceptable use policy, regardless of its real or apparent origin.

Procedural Issues Relating to Access to Systems. DAS 03-21 provides that "The agency may withdraw permission for any or all personal or business uses of its system at any time without cause or explanation. No one shall grant access to systems without agency authorization."

Consistent with university disciplinary procedures and state and federal law, and as a reasonable part of managing limited resources in furtherance of the University's mission, your access to systems may differ from the access granted to others. For example, the UO electronic information systems you are authorized to access may vary with your job responsibilities, research you are conducting, courses you are taking, or other objective factors. Moreover, the access you may be granted is access personal to you, and not access that is transferable, assignable, or sharable. Thus, for example, you may not give your username and password to a relative, or loan a friend your microcomputer lab pass.

It is important that you also realize that connection of a personally owned or controlled system to a University owned or controlled resource (such as UOnet) may substantially impact what constitutes permissible access to, or use of, that system. For example, permissible uses of a student owned microcomputer would normally be solely subject to that student's personal priorities and judgments; once that microcomputer is connected to UOnet, however, the situation changes. Once that system is connected to the

network, the student could potentially run that microcomputer as a multiuser timesharing host, and could potentially grant virtually unlimited access to University resources (such as network bandwidth, domain-name-limited licensed resources such as electronic publications, etc.); clearly, such use would be contrary to the fundamental rule governing access to University resources, namely that access is not transferable, assignable, or sharable.

7. Privacy Expectations [DAS 03-21: "Public Records Are Controlled By the Agency"]

The University recognizes its responsibilities to preserve and retain public records. The University also recognizes the need to provide an environment that

- respects the legitimate need and desire for faculty, staff, and student privacy, and
- facilitates collaboration with corporate, governmental, and non-profit agencies on topics of mutual interest, including topics that may be subject to voluntary non-disclosure agreements ("NDAs"), contractual trade secret restrictions, govern-mentally-imposed security restrictions, or other limits on information disclosure or retention.

Application of those principles to University electronic information systems has the following general implications:

- User-created files or electronic messages that are solely personal in nature shall not be treated as public records, provided, however, that authorized University staff may access such materials as allowed by section 6 herein.
- Even such non-public records may be disclosed to proper authorities upon receipt of an enforceable warrant or subpoena for those records.
- Disclosure of files or messages containing evidence of criminal activity may voluntarily be made to law enforcement officials if incidental/accidental contact with the content of those files or messages occurs, and the incidental/accidental contact reveals patently un-lawful conduct (for example: a misaddressed mail message is received containing a list of stolen credit card numbers, a cache of pirated software is discovered while resolving a systems problem, an operator notices child pornography printing on a shared printer, etc.).

8. Public Impressions and Your Online Style [DAS 03-21: "Uses Must Reflect the Agency Image"]

DAS 03-21 states that "Uses of agency systems do not all have to be formal. But, they must be professional. For example, e-mail must look like state e-mail, not the product of a pop culture. Authors must not use CB handles or pen names, personal symbols, ornamental quotes, or newsgroup or chatroom slang."

As permitted by DAS 03-21, the University elects to adopt a different policy with respect to this issue:

We all know that the behavior and conduct of all University of Oregon faculty, staff and students contributes to, or can detract from, the University's overall public image, online as in day-to-day encounters.

The University relies on and trusts its faculty, staff, and students to exercise good judgment in what they say and how they say it, including adapting their normal usage and style to what is most appropriate for the circumstances at hand. We recognize that this may mean using technical nomenclature or popular slang in order to best communicate with some audiences, while in other circumstances standard formal written business usage may be most appropriate.

Because of the unexpected longevity of online communications; the fact that electronic communications suffer from lack of access to customary communication cues such as inflection, tone, and body language; the reality that some electronic correspondents may not speak English as their primary language; the difficulty of correcting initial misimpressions online; and the ease with which someone may elect to ignore your online communications entirely should they wish to do so, you may want to employ a more careful and restrained writing style than you normally would, despite the apparent informality of online communications.

With respect to use of nicknames, personal symbols, ornamental quotes, or other material that is sometimes included in signature files, we ask that you consider the fact that signature files can be either helpful or overused/abused to the point of being a cliche. If you correspond with someone frequently, your use of a long or particularly ornate signature file may serve only to annoy your correspondent and mark you as a novice online. As you grow accustomed to working with people online, you will come to see that there is often a strong relationship between online competence and the length of one's signature file, with the most competent users having particularly succinct signature files, if they use one at all. (In general, a signature file longer than four lines should be scrutinized by the user and edited to meet that generally accepted network norm.)

9. Personal Responsibility for Online Statements [DAS 03-21: "Uses Must Be Lawful and Inoffensive"]

This section of DAS 03-21 provides in part that "Uses of agency systems must not be false, unlawful, offensive, or disruptive. Unless agency duty requires it, no use shall contain profanity, vulgarity, sexual content, or character slurs. No use shall make rude or hostile reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability."

We affirm by this document that University of Oregon electronic information systems may not be used for unlawful purposes, including discriminatory conduct against protected classes of individuals or hate crimes.

In all cases, you are personally responsible for what you say, write, or do. For example, if you defame someone online or invade his or her privacy, you may be sued; if you engage in sexually harassing behavior online, you may be subject to the penalties for that offense.

We trust in the process of civil intellectual discourse. If you make false utterances, the free and open clash of ideas will inevitably expose those false utterances to the glaring light of public scrutiny and rejection. If you commonly make offensive or vulgar remarks, your crude expressive style will mark you as an uncultured person whose ideas deserve little if any consideration.

10. Academic Freedom, Freedom of Expression, and Prior Review [DAS 03-21: "Publishing Must Be Agency Authorized"]

DAS 03-21 provides in part that: "All publishing is restricted to state business as described by the agency. All publishing requires agency authorization."[1]

We recognize that publication and public presentation of materials is an integral, non-segregable part of academic life, and that a typical faculty member will generate scores of articles, and routinely author books, monographs, essays, and electronic communications, etc.

It would be impractical and unprecedented for the University to require prior review and approval of all academic materials submitted by University affiliates for publication or public presentation, and we do not elect to do so, since existing peer review channels provide a timely and consensually recognized means by which publications can be assessed.

At the same time, it is the University's right and prerogative to designate specific University officials to work with media representatives, legislators and officials of government in communicating the University's official position on matters of interest. No one shall hold him/herself out as an official representative of the University, speaking on its behalf, unless that person has been authorized by the University administration to do so.

In circumstances where a reasonable observer might become confused and believe that the speaker is articulating or presenting an official University of Oregon position, when in fact the opinion or content expressed or displayed is purely personal, the speaker or writer shall include an appropriate disclaimer clarifying the status of his or her comments, presentation, or display.

DAS 03-21 also states that "Many Internet or e-mail groups exist to share useful information. The agency may authorize a user to post queries or to represent it by posting professional comments to useful groups." We hereby authorize University faculty, students, and staff to do so, subject to the disclaimer requirements of the proceeding paragraph, and subject to the charter and/or prevailing norms of those fora. This paragraph shall not be deemed to authorize or permit off-topic postings made with disregard to a mailing list or newsgroup's underlying purpose, excessive crossposting of articles, mass posting of the same article to multiple newsgroups on a group-by-group basis, or the sending of commercial e-mail.

11. Permitted Personal Uses of Electronic Information Systems [DAS 03-21: "Personal Uses Restricted"]

DAS 03-21 explicitly permits certain personal uses of electronic information systems, while excluding all personal uses that are not explicitly permitted.

We explictly disallow only certain personal uses of non-administrative electronic information systems, and permit all others (subject to future exclusion). Particular points where we differ from DAS 03-21 are outlined below.

Personal Toll Calls. University employees should use a personal telephone credit card to make personal toll calls. In circumstances where a personal telephone credit card is inconvenient or unavailable, a reasonable number of personal toll calls may be made on University telephones, with departmental approval. In such situations, a log of the calls must be maintained and prompt reimbursement tendered at the next appropriate billing cycle.

Cellular Phones. Cellular telephones and services are provided to certain University of Oregon employees to conduct activities incident to their University employment. University cellular telephones may not be used to make personal calls that result in charges being billed to state accounts, even when the employee intends to reimburse the University for the charges. Likewise, an employee may not operate a personal business from a University cell phone.

Managers and supervisors are responsible for educating and monitoring subordinates' cellular service usage. In emergency situations, managers may grant exceptions to these usage policies. In such circumstances, any charges must be reimbursed by the employee on a timely basis.

Copying. Employees may make a reasonable number of personal photocopies, provided the employee's department approves and reimbursement is made.

Personal Web Pages. Personal Web pages are permitted, provided the pages are non-commercial and otherwise consistent with the University's Acceptable Use Policy and this document.

Use of "cgi-bins" and "server side includes"[2] may be restricted or enjoined to protect system performance, maintain system security, or in furtherance of other University or departmental objectives.

Disk quotas may be employed where appropriate to insure that disk space used for personal Web pages is kept to reasonable limits. Personal pages that require disproportionate network or system resources may be disallowed, regardless of content, although departments are urged to

---

[1] "Publishing" is explicitly defined in DAS 03-21 as meaning "using systems to disseminate or spread information to the public or beyond the user's area of authority within the agency. Examples include newsletters, Web pages, fliers, chain letters, and postings to Internet groups or e-mail lists."

[2] "Cgi-bins" are computer programs or scripts that are executed when a Web page is accessed; for example, access (or 'hit') counters are often implemented as a cgi-bin, as are guestbooks and programs designed to process HTML form input.

"Server-side includes" are closely related to cgi-bins in that they automatically execute tasks when a Web page incorporating a server-side include is accessed. For example, a Web page with a server-side include might send an e-mail message whenever that page is accessed, or it might cause the latest version of a standard boilerplate copyright notice to be automatically included at the bottom of the document.

recognize and support particularly meritorious pages to the extent that resources and other higher priority system uses permit.

It is inappropriate for any third party organization's primary Web pages[3] to be served from a University Web server, even if such pages are offered on a volunteer basis without remuneration and with no commercial content thereon; exceptions to this policy need to be approved by the University.

"Banner exchanges" that include commercial sites are inappropriate on personal Web pages due to the commercial nature of their content. Links to commercial sites that are intrusive or that facilitate marketing or promotion rather than serving as a simple link to another site are inappropriate due to their commercial content.

Postings to Internet Newsgroups and/or Electronic Mailing Lists. Postings to Internet newsgroups or electronic mailing lists shall be permitted, provided that the posting's content is lawful, is on-topic with respect to the group or groups to which it is posted, is not excessively crossposted (or posted multiple times), includes a disclaimer if there is any possibility the posting might be mistaken as an official University pronouncement, and is otherwise consistent with prevailing norms for the fora to which it is posted.

The University reserves exclusive right to manage the propagation of newsgroup postings in all respects, and cannot accept responsibility for postings that do not propagate, or postings that propagate incompletely.

Postings that include copywritten material shall only be made with the express permission of the copyright holder.

User postings made to UO news servers may not be made with altered, forged, or suppressed **From:** lines.

Users may not add **Approved:** headers to postings made to moderated newsgroups for which they are not the moderator.

Only University-authorized news administrators shall issue newsgroup control messages; individual users may issue control cancel messages for articles of their own that they desire to cancel.

Use of Electronic Information System for Advocacy Purposes. Any use of electronic information systems for advocacy (DAS 03-21 uses the term "personal soliciting") shall be permitted only if it is minor/incidental in nature, non-disruptive, and clearly disclaimed as a matter of personal opinion rather than University policy. For example, it would be inappropriate for a candidate for public office to publish campaign-related material from a University Web page, or for a University affiliate to send a mass electronic mailing advocating a particular social, political, or religious position to hundreds of people who haven't requested information on that topic.

Connection of Personally Owned Devices To State Owned Devices. In some cases, employees may elect to privately provide a device to augment or enhance the capabilities of a state owned electronic information system. For example, an employee might bring a personally-owned printer or an ergonomic keyboard to work, and connect it to a state-owned microcomputer. Such activity shall be permitted, provided the employee's department agrees to such connection, the personally-owned property is clearly marked, the state-owned property is unharmed by the interconnection, and the personally-owned property is segregable with minimal effort in the event the employee leaves that office, interoperability problems arise, or other circumstances require discontinuance of approval for use of the personally-owned device.

Installation or Downloading of Software. DAS 03-21 provides that "Users may not install or download software without agency authorization." By this section, the University of Oregon authorizes the installation or downloading of software, provided

- such software has been lawfully acquired and is under an appropriate license (or is freeware, or is shareware used in accordance with the shareware program author's usage limitations);
- the software does not interfere with system operations, systems integrity, or the functioning of other software; and
- said software installation or download has not been prohibited by the user's department or the department having authority over the equipment being used.

Thus, for example, a faculty member could purchase and install a new statistical program on a state owned microcomputer installed in her office unless her department prohibited such installations. Another example: if a student-access microcomputer lab has a policy prohibiting installation of new software or tampering with existing software, users of that lab may not download and install a program they acquired from an FTP site or Web site.

Hours for Personal Use of Electronic Information Systems. DAS 03-21 states that "Personal use must be done during meal and rest breaks; not before, after, or during work."

[3] Web pages shall be considered the primary Web pages for an organization or entity if there is no other authoritative site for that organization or entity, or if in balance, the other site has less (or less authoritative) content regarding that organization than does the UO-based site.

Our position is somewhat different. University faculty and staff often do not have fixed meal and rest break times, and by definition, the campus work day may begin early and continue late into the evening, with the work day broken into several non-contiguous blocks of time. Moreover, we as an institution believe that channeling use of electronic information systems into meal and break times could increase the likelihood of equipment damage from spilled food and drink.

Our expectation for personal use of electronic information systems is that usage will be before work, or during otherwise unproductive lulls (for example, while waiting for programs to compile), and that any use that interferes with accomplishment of a user's assigned responsibilities will be discontinued at once.