University of Oregon
Acceptable Use Policy for Information Technology Resources

REASON FOR POLICY

This Policy establishes the acceptable use of computing and other technology resources and facilities ("IT resources") at the University of Oregon ("UO").

PERSONS AFFECTED BY THIS POLICY

All persons who use UO IT resources, including UO employees, students, contractors, vendors, guests, and any other user allowed access to UO IT resources.

WEBSITE ADDRESS FOR THIS POLICY

[XXXXXXXXXXXXXXX]

RESPONSIBLE OFFICE

For questions about this policy, please contact the Chief Information Security Officer at 541-346-9700 or ciso@uoregon.edu.

ENACTMENT & REVISION HISTORY

This Policy replaces the "UO Acceptable Use of Computing Resources Policy" (https://it.uoregon.edu/acceptable-use-policy). This Policy also replaces the "University of Oregon Acceptable Use of Computing Resources" Addendum (https://it.uoregon.edu/aup-addendum) to the Oregon Department of Administrative Services' Statewide Policy on Acceptable Use of State Electronic Information Systems (DAS 03-21), dated February 20, 1997.

POLICY

1.0 Overview

This policy is intended to further UO's educational, instructional, research, and administrative activities, and promote free and open inquiry and discussion, while acknowledging that UO IT resources are government property and therefore subject to certain restrictions. This policy is also intended to help ensure fair allocation of IT resources to avoid needless disruption.

Under ORS Chapter 352, UO is a government entity performing governmental functions and exercising governmental powers, and UO IT resources are UO property. Further, UO owns

information stored on UO computer systems, such as email containing UO administrative data, communications pertaining to UO business, and other proprietary information.

In general, UO IT resources may be used only for UO business related activities. Furthermore, information related to UO business activities ~~are~~ is subject to the Oregon Public Records Law. ~~and~~ UO employees have ~~no expectation of privacy in such information except as specifically recognized by law~~an expectation of privacy in their email communications.

> *TF NOTE: Preservation of areas of privacy is fundamental to free speech and academic freedom and to the work of various employees. Various universities impose explicit restrictions on university access to faculty, staff, or student email, rather than simply declaring (in a document nobody will ever read) that there is no privacy in emails. See, for example: (North Carolina - http://policies.unc.edu/policies/electronic-privacy/; Berkeley - https://security.berkeley.edu/email-service-policy).*

Employees may make incidental personal use of UO IT resources in compliance with this Policy and other UO policies. ~~Incidental and limited personal use of UO IT resources by employees may be permitted if it is minimal, does not interfere with UO's or the employee's ability to carry out UO business, and does not violate terms of this policy, other UO policies, or applicable state and federal law.~~

> *TF NOTE: "Incidental" is a sufficient restriction, without adding "limited," which has no definition in the policy. As for Interfering with employee's work, that is covered under section 4.2. As for not using IT resources to violate laws, policies, etc., that is already covered under those laws and policies, so is not needed here.*

Users of UO IT resources may have access to valuable UO resources, to sensitive data, and to internal and external networks. It is therefore essential that all users behave in a responsible, ethical, and legal manner.

2.0 Objective / Purpose

The purpose of this document is to outline acceptable uses of UO IT resources, ~~and~~ to educate users about their individual legal and ethical responsibilities when using those resources, and to create obligations that can lead to punishment of users.

> *TF NOTE: The addition is more honest and may draw more attention to the policy.*

This policy is not intended to preclude uses of UO IT resources that are specifically authorized by Collective Bargaining Agreements to which UO is a party.

3.0 Scope

This policy is directed to all UO employees, students, contractors, vendors, guests, and any other user with authorized access to UO IT resources. It applies to all users of UO IT resources and data, whether affiliated with the UO or not. It applies to all use of those resources and data,

whether on campus, via cloud-based servers, or from remote locations (e.g., through a virtual private network or "VPN"), and covers all devices attached to UO's network, whether via a UO-owned computer or device or one personally owned by the individual.

4.0 Appropriate Uses

4.1 UO IT resources are provided for UO business-related purposes, including support for the UO's teaching, research, and public service missions, its administrative functions, and student and campus life activities.

4.2 Employees may make incidental personal use of UO IT resources in compliance with this Policy and other UO policies. Such use ~~must be minimal, and~~ cannot interfere with the fulfillment of that employee's job responsibilities or disrupt the work environment or the UO's ability to carry out UO business. ~~Personal use that inaccurately creates the appearance that UO is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.~~ Statements or expressions made in personal use do not represent positions or expressions of the University. As such, a user shall not intentionally assert that he or she is endorsing, supporting, or affiliated with any organization, product, service, statement, or position on behalf of the University unless authorized.

TF NOTE: It is sufficient to ensure that personal use does not interfere with work. The undefined word "minimal" is both unneeded and liable to abuse. Prohibiting personal use that "creates the appearance" that the UO is endorsing a product uses a subjective standard, potentially makes satire a cause for dismissal from the University, and is unnecessary.

4.3 Students may make personal and academic use of personally owned computers using UO IT resources in compliance with this Policy and other UO policies.

5.0 Compliance with Federal and State Laws and UO Policies: All users of UO IT resources must:

5.1 Abide by all federal, state, and local laws, regulations, rules and UO policies, including, for employees but not for non-employees, while on the job during work hours, ~~but not limited to~~ ORS Chapter 260.432, which~~laws that~~ during such times precludes public resources from being used for political campaigning on behalf of or in opposition to a candidate in an election or on behalf of or in opposition to a measure that has been certified for a ballot ~~under ORS Chapter 260.432~~.

TF NOTE: The original version did not accurately reflect Oregon law. ORS 260.432 controls only employees, only email during work hours, and only emails that constitute political campaigning regarding candidates in an election or ballot measures in an election.

5.2 Abide by all software contracts and licenses applicable to their particular uses. The UO has entered into contracts for many of its software and network resources which require each individual using them to comply with those agreements.

5.3 Abide by federal copyright laws when using UO IT resources. ~~Do not use, copy, or distribute copyrighted material unless you have a legal right to do so.~~ The unauthorized use or publishing of copyrighted material with UO IT resources is prohibited~~, and users are personally liable for consequences stemming from such unauthorized use~~.

TF NOTE: The "Do Not Use" sentence is not a regulatory sentence but merely hortatory. The last phrase appears to create personal liability to someone (who?), but such liability is a matter of law, not of UO policy.

~~**5.4** Refrain from using UO IT resources for commercial purposes or any other private financial gain, except as authorized in writing pursuant to UO's conflict of interest and outside employment policies~~

TF NOTE: This is a vague reference to something or other, without proper citation to UO policies by number. The "conflict of interest policy" (adopted by the Senate) does not prohibit employees from pursuing private financial gain (whether through IT resources or otherwise) and does not require written permission for most outside work. There is no UO policy titled an "outside employment policy." Faculty members are allowed to engage in outside work (including for private financial gain) without any approval – written or otherwise. Such outside work has long been explicitly authorized by the one-day-per-work-week (plus weekends) policy. For students, there are no prohibitions whatsoever, yet this purported to apply to "all users."

5.5. Refrain from using electronic mail systems for ~~broadcasting any unsolicited email or for~~ any purpose prohibited by federal or state law.

TF NOTE: The deleted language is vague ("broadcasting"). Is it a "broadcast" to send a message to a listserv of philosophers, for example? To prohibit broadcasting an "unsolicited email" apparently would prohibit faculty members from sending group emails to the listserv if the recipients haven't first "solicited" the email – whatever that means.

6.0 Policy Requirements: All users of UO IT resources:

6.1 Shall not use UO IT resources without proper authorization. All users must use only those IT resources that they are authorized to use and use them only in the manner and to the extent authorized.

6.2 Shall not use UO IT resources to attempt unauthorized use, or from assisting in, encouraging, or concealing from authorities any unauthorized use (or attempt at such use), or to willfully interfere with other individuals' authorized uses of any UO computer or network facility.

6.3 Shall not purposefully endanger or circumvent the security or security mechanism of any UO IT resource. All users must also refrain from any attempt to degrade system performance or capability, damage systems or intellectual property of others. Users shall not create, install, or knowingly distribute a malicious program that interferes with the confidentiality, integrity or availability of data on any computer or network facility.

TF NOTE: The insertion to ensure that endangerment is purposeful is important. Otherwise, people would accidentally violate 6.3 when they get a virus. That is not their fault.

6.4 Shall not connect any device which processes sensitive data, as described in the Data Classification Policy, to any of UO's IT resources (including but not limited to its networks) unless the device meets technical and security standards set by UO procedures.

TF NOTE: Technical change.

6.5 Must fairly utilize shared IT resources in accordance with Unit policies and/or procedures set for the computers involved and cooperate fully with the other users of the same equipment.

6.6 Shall not use UO IT resources to transmit any communications that reasonably ~~could be considered obscene or threatening or constituting prohibited discrimination (including discriminatory harassment) by the recipient or another viewer, as defined by federal and state law and UO policy.~~ violates UO Policies, keeping in mind that prohibitions in such Policies are subject to the freedom of expression provisions of Article I, section 8, of the Oregon Constitution, the First Amendment to the U.S. Constitution, and UO Policies on Freedom of Speech and Academic Freedom. For more information on UO policies in this area, see ~~the Office of Affirmative Action & Equal Opportunity web site~~http://policies.uoregon.edu.

TF NOTE: (1) The sentence to be deleted uses vague and subjective language, exposing faculty, students, and staff to potential punishment without proper notice. In addition, its terms go beyond what is allowable under the Constitution of the State of Oregon as interpreted by the Supreme Court of Oregon. The University cannot impose policies that contradict the Oregon Constitution. (2) Rather than introducing new, subjective language, it is better to refer simply to violation of "UO Policies." (3) It is important to keep in mind the superior authority of two Constitutions and two other important UO Policies (speech and academic freedom).

6.7 Shall not share a password for a Duck ID, or use another person's Duck ID password. Users will also not perform or pursue unauthorized viewing, use, alteration or deletion of another person's computer files, programs, and accounts, or electronic records. Access to such information does not imply permission to view or use it. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. In situations where records of another user need to be accessed, please see the Electronic Records Access Procedure."~~Shall not share a password for any UO IT resource or use another person's password. This includes unauthorized viewing, use, alteration or deletion of~~

~~another person's computer files, programs, and accounts, or electronic records. Access to such information does not imply permission to view or use it. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. For more information, please see the Electronic Records Access Procedure.~~

TF NOTE:

6.8 Shall not misrepresent their identity or relationship to the UO when requesting access to or using UO IT resources. Furthermore, ~~no~~ users shall ~~hold themselves out as an official representative of UO, speaking on its behalf, unless that person has been authorized by the UO administration to do so~~comply with the provisions of Section 1(d) of the Academic Freedom Policy of May 28, 2014, which states that "university community members have the right to identify their association or title, but should not claim to be acting or speaking on behalf of the University unless authorized to do so." ~~In circumstances where a reasonable observer might become confused and believe that the speaker is presenting an official UO position, when in fact the content or opinion expressed or displayed is personal, the speaker or writer shall include an appropriate disclaimer clarifying the status of their comments, presentation, or display.~~

TF NOTE: The second sentence's language is similar to the language of the Academic Freedom Policy of May 28, 2014, but introduces new, vague terms such as "hold[ing] oneself out," "official representative," and "authorized by the UO administration." Instead of making new policy, it is better simply to refer to the exact language of existing policy.

As for the last sentence, the language is subjective and would contradict the Academic Freedom Policy of May 28, 2014, which provides an objective standard. The AF Policy is objective, because it is a simply permission and a prohibition, which anyone can understand and on which discipline can be based. In contrast, the language I suggest deleting can subject to discipline a faculty member, student, or staff member if a "reasonable observer" "might become confused" and might "believe that the speaker is presenting an official UO position," unless the speaker or writer includes "an appropriate disclaimer." The language in the AF Policy is not only objective instead of subjective, but prevents punishment based on someone's assumption of whether a "reasonable observer" might become confused, etc.

6.9 Shall not physically modify ~~or reconfigure~~ any UO-owned computer or ~~any~~ devices connected to the UO network facility without proper authorization.

TF NOTE: Employees and students reconfigure and modify their computers with every usage – every time they save a file, install software, or adopt a new browser add-on. This needs to be deleted b/c it places everyone in constant violation or substantially modified.

6.10 ~~Users shall take full responsibility for UO data that they store on computers and transmit through network facilities.~~ No one shall use computers or network facilities to store, share, or

transmit UO data in ways that are prohibited by law or UO policy. More information on how data is classified at UO can be found in the Data Classification Policy.

TF NOTE: What does "take full responsibility" mean?

6.11 Those who publish web pages on UO owned or administered IT resources ~~shall take full responsibility for what they publish and~~ shall respect the acceptable use conditions for the computer or resource on which the material resides. References and links to commercial sites are permitted, but ~~advertisements, and especially~~ paid advertisements~~,~~ are not. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar information resources.

TF NOTE: What does "take full responsibility" mean? Delete b/c vague and introduces a questionable concept of "unpaid advertisements". If one puts a link to a colleague's book on my UO website recommending it, is that an advertisement? Possibly it could be construed as such. It should not be disallowed.

6.12 Users of UO IT resources shall comply with the regulations and policies of UO-hosted mailing lists, social media sites, and other public forums when making use of those lists, sites, and forums.

TF NOTE: Obvious, but needs to be here. Otherwise it is technically saying we all need to comply with those all the time.

6.13 System administrators shall refer all disciplinary and legal matters to appropriate authorities.

6.14 Email and other electronic messaging technologies are intended for communication between individuals and clearly identified groups of ~~interested~~ individuals, not for mass broadcasting. (For more information, see Guidelines for Official Mass Email.) UO reserves the right to discard ~~incoming mass mailings,~~ messages containing malware~~,~~ and spam without notifying the sender or intended recipient. UO also reserves the right to block communications from sites or systems that are involved in extensive spamming or other disruptive practices.

TF NOTE: Sometimes users want to receive mass mailings because some groups don't use listservs but cc or bcc lists.

6.15 No individual or group may establish or extend network connectivity without prior authorization and discussion with the Information Services Network team.

6.16 As a general matter, UO does not monitor individual usage. Users should be aware that under many circumstances, and as consistent with law, uses of UO IT resources are not private. ~~However, users should be aware that their uses of UO IT resources are not private.~~ The UO Information Security program has adopted a procedures document that, among other things, authorizes Deans, Department Heads, and other managers to view employee emails

and other usages (including telephone records) under various circumstances. This document is titled "Information Services Procedures for Accessing Employee Electronic Communications Records," although it contains not only "procedures" but also policies allowing monitoring. See https://is.uoregon.edu/system/files/UO_IS_ElectronicRecordsAccessProcedure.pdf.

TF NOTE: The first change is more accurate. The second is added to inform users that department heads and deans can sometimes read their emails, which is in the cited policy.

Furthermore, records created, owned, used or retained that relate to the conduct of the public's business are subject to the Oregon Public Records Law.

TF NOTE:

Under certain defined circumstances, UO reserves the right to monitor the normal operation and maintenance of all IT resources including backup, logging of activity, general usage patterns, and other activities as necessary to evaluate and maintain information security, efficiency, and delivery of service. Specific to Security monitoring, in Section 4 of the Information Security Program, "the Information Security Office will not investigate monitored data at the level of an individual user, but will investigate at the individual level when an appropriate triggering event occurs on its Security Systems (such as the antivirus system)."

TF NOTE: The additional information is more informative.

7.0 Enforcement and Implementation

7.1 Roles and Responsibilities

Each UO employee, UO student, ~~and~~ department/unit, or other user is responsible for complying with this policy. The Office of the Chief Information Security Officer is responsible for enforcing this policy, and is authorized to create technical and security standards for UO IT resources and protection standards for information stored or transmitted by UO IT resources.

TF NOTE: The policy says in section 3 that students are also covered. And section 7.2 makes this explicit. So they should not be excluded here.

7.2 Consequences of Noncompliance

Violations of this policy may result in the same types of disciplinary measures and consequences as violations of other UO policies, in accordance with applicable UO policies, procedures, and Collective Bargaining Agreements, or, with respect to students, the Student

Conduct Code. In some cases, violations of this policy may also constitute violations of state and federal laws, and consequences may include criminal prosecution.

Systems and accounts that are found to be in violation of this policy may be removed from the UO network, disabled, etc., by the Unit or Information Services as appropriate until the systems or accounts comply with this policy.

8.0 Definitions

UO IT Resources – all computers (including but not limited to servers, desktops, laptops, phones, and any networked device that provides computational services) and software owned or paid for by the UO, including departmental computers, cloud-based services, and the UO's computer network facilities. ~~all computers (including but not limited to servers, desktops, laptops, phones, and any networked device that provides computational services) owned or administered by any part of the UO or connected to the UO's communication facilities, including departmental computers, cloud-based services, and all of the UO's computer network facility accessed by anyone remotely (such as using a VPN).~~

TF NOTE: Edited for clarity and simplicity.

Proper Authorization – permission granted by technical staff after consulting managerial staff and the terms of this Policy. For unit-level issues, this would include authorization by IT Professional staff, after consulting management in the unit. For campus-wide issues this would be authorization by Information Services.