

CHAPTER 11 - INFORMATION TECHNOLOGY

ACCEPTABLE USE OF COMPUTING AND TELECOMMUNICATIONS RESOURCES No. 11-20-010

Effective Date: January 10, 2006

1. Applicability

This policy applies to all users of University computing, telecommunications and wireless resources, including but not limited to computers, computer systems and networks, portable digital assistants (PDA's), telephones, pagers, cellular phones and two-way radios, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations. These resources are hereinafter referred to as "computing and telecommunications resources." Additional guidelines may be established by OHSU to apply to specific computers, computer systems, networks or applications.

2. Requirements

A. Legal

A user of University computing and telecommunications resources shall comply with all federal, Oregon, and other applicable laws; all generally applicable University rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; Federal Communication Commission regulations; the University's Code of Conduct; the University's sexual harassment policy; and all applicable software licenses. Users who engage in communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

B. Authorized

A user of University computing and telecommunications resources shall use only those resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before accessing any computing resources.

Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.

A user of computing and telecommunications resources shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access other persons' accounts does not, by itself, imply authorization to do so.

C. Reasonable

A user of computing and telecommunications resources shall respect the finite capacity of those resources (including, for example, bandwidth, disk space and CPU time) and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

D. Personal

A user of computing and telecommunications resources shall not use those resources for personal commercial purposes or for personal financial or other gain, except as may be authorized under [Policy No. 10-01-015](#) (Outside Activities/Outside Compensation policy) or institution established news groups.

Incidental personal use of computing and telecommunications resources for other purposes is permitted when the use:

- (1) does not unreasonably consume those resources;
- (2) does not interfere with the performance of the user's job or other University responsibilities;
- (3) does not consume an unreasonable amount of the user's time;

(4) does not concern subjects inappropriate in a work or study environment (e.g. accessing pornographic web sites);

(5) is not inconsistent with OHSU's mission of healing, teaching and discovery; and

(6) is otherwise in compliance with this and other OHSU policies including requirements to reimburse the University where required under [Policy No. 03-25-080\(2\)](#).

Further limits may be imposed upon personal use in accordance with normal supervisory responsibilities.

E. E-Mail and OHSU Communications

E-Mail and calendar systems are designed to facilitate the communication of business ideas and materials pertinent to the operation of the University.

Announcements, bulletins, and documents deemed by management to be of value and interest to the well-being of employees are an integral part of the system. Except as otherwise authorized by collective bargaining agreements or by Employee Communications, all broadcast e-mail (unsolicited messages sent to more than 50 OHSU addresses across departments) must be submitted and approved by Employee Communications and shall be distributed during off-hours by ITG.

Communications over the e-mail system shall be professional and appropriate for the workplace or group setting. E-mail may not be used for personal solicitations or advertising or other activities except through OHSU provided electronic news group systems for those types of activities. Propagation of chain letters is specifically prohibited.

Falsifying e-mail headers (e.g. providing a false sender's address) or routing information so as to obscure the origins of mail or mail routes is forbidden. Altering the content of a message attributed to another is not permitted unless the changes are explicitly noted.

F. Representing the University

A user of computing and telecommunications resources shall not state or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so. Affiliation with the

University does not, by itself, imply authorization to speak on behalf of the University. Authorization to use University trademarks and logos on computing and telecommunications resources may be granted only by University News and Publications. The use of appropriate disclaimers is encouraged.

3. Security

The University employs various measures to protect the security of its computing and telecommunications resources and of their users' accounts. Users should be familiar with OHSU information security practices and engage in applicable "safe" practices, for example, by establishing appropriate access restrictions for their accounts, keeping the network virus-free, safeguarding passwords, ensuring proper physical safeguards, and protecting the confidentiality of electronic protected health information.

4. Expectation of Privacy

A. General

University computing and telecommunications resources are not private. For example, communications made by means of these resources are subject to Oregon's Public Records Law to the same extent as they would be if made on paper. The normal operation and maintenance of the University's computing and telecommunications resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

B. Reason to Access Activity

In addition, the University may access or monitor the activity and accounts of individual users of University computing resources, including individual log in sessions and communications, without notice, when:

- (1) The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
- (2) It is necessary for OHSU work and business-related reasons (e.g. a person is on vacation or sick leave and access to some files is needed to further institution business);

(3) It reasonably appears necessary to do so to protect the integrity, confidentiality, availability, or functioning of the University generally or computing and telecommunications resources in particular, or to protect the University from liability;

(4) There is reasonable cause to believe that the user has violated, or is violating, OHSU policy;

(5) An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or

(6) It is otherwise required by law.

Any such access or individual monitoring, other than that specified in 4. A. and B.(1) above, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by three of the following individuals: Vice president of Human Resources, Legal Counsel, Chief Information Officer, and Information Security Officer. The head of the unit which employs the individual will be notified of such access when appropriate. The University, at its discretion but subject to any applicable laws, may disclose the results of any access or monitoring, including the contents and records of individual communications, to University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings and/or legal proceedings.

C. Monitoring as a Job or Service Requirement

The University may also authorize access and monitoring of an employee's or agent's actual communications over its computing and telecommunications resources where customer service is a primary responsibility of an employee's job duties. Such monitoring must be authorized by the Vice President of Human Resources and employees in positions subject to monitoring shall be notified of such activity.

5. Remote Access to OHSU Computing Resources

A. OHSU employees and students may be authorized secure remote access to information assets owned by or in custody of OHSU. Remote access may be granted by the department director or other appropriate authorizing authority where appropriate to fulfill a person's work or other responsibilities.

B. Remote access for contractors, business partners, referring physicians, other health care providers or other approved users with significant business justification may be approved on a case-by-case basis by an appropriate authorizing authority.

C. Applicants for remote access must submit the OHSU Remote Access form. Information technology support vendors may also be granted remote access for system and application maintenance as negotiated in the support contracts.

D. Noncompliance with the requirements of a remote access authorization or with other provisions of this policy, as determined by the authorizing authority, may result in immediate loss of access privileges and possible corrective or legal action against the violator.

6. Enforcement

Users who violate this policy may be denied access to computing and telecommunications resources and may be subject to other penalties and disciplinary action, both within and outside of the University. Violations will normally be handled through the University procedures applicable to the relevant user. However, the University may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so to protect the integrity, confidentiality, or availability of University or other computing resources, or to protect the University from liability.

Background: formerly Policy No. 08-20-010 (renumbered)

Implementation date: June 23, 1998

Revision dates: March 1, 2001; August 8, 2001; January 10, 2006

Related policies, procedures and forms:

Policy No. 01-05-010, [Confidentiality](#)

Policy No. 01-05-012, [Confidentiality of Health Information](#)

Policy No. 03-25-080, [Use of Institutional Resources](#)

**Policy 10-01-015, [Outside Activity/Outside Compensation Policy](#)
Network Services Usage Agreement
OHSU Remote Access Form
Service Observation [\(Quality Monitoring\) Form](#)
Responsible office: Integrity Office**