OREGON INSTITUTE OF TECHNOLOGY

Computer Use
OIT-30-005

Objective

To ensure Oregon Institute of Technology (OIT) and all OIT users are protected from illegal and/or harmful actions that may result from inappropriate use of OIT computer resources; and to inform users of their responsibility in the use of OIT computer resources.

Use of Computer Facilities

The use of OIT computing resources is for purposes related to the university's mission to deliver a quality education and support technology that meets the needs of all users and the organization. Users are entitled to use the university's computing resources only for purposes related to their studies, instruction, the discharge of their duties as users, their official business with OIT, and other university-sanctioned activities. Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, users should consult ITS personnel for clarification.

User Responsibilities

Violation of the OIT Computer Use Policy may result in suspension and/or termination of computer privileges.

1. Users assume personal responsibility for the use and security of their accounts. Users may not disclose their passwords or otherwise make OIT's facilities available to unauthorized individuals.
2. Users are responsible for the security, privacy, and control of data in their care, access privileges entrusted to them, and their username and password. Users must use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.
3. The possession or collection of passwords, personal identification numbers (PINs), private digital certificates, or other secure identification information belonging to other users is prohibited.
4. Use of any OIT-owned computer or network for private, commercial, non-OIT business purposes without explicit authorization is a violation of these terms and conditions of use and could result in the termination of computer privileges.
5. Computer facilities have tangible value. Attempts to circumvent accounting or information systems or to use the computer accounts of others (e.g., use of rogue wireless access points) will be treated as forms of attempted theft.
6. Users are prohibited from installing, storing or using unlicensed software on OIT computers. Transmission of such software over the OIT network is prohibited.
7. The introduction of data or programs which in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program), or which infringes upon the rights of other OIT users (e.g., inappropriate, obscene, pornographic, bigoted, or abusive materials) is prohibited.
8. Users may not attempt to circumvent security systems or to exploit or probe for security holes in any OIT network or system, nor may users attempt any such activity against other systems accessed through OIT's facilities. Execution or compilation of programs designed to breach system security is prohibited unless authorized in advance.

Privacy and Monitoring

The use of OIT computing resources is not completely private. It is the policy of the university not to monitor individual usage of computing resources. However, OIT reserves the right to monitor and record the usage of all computing resources as necessary to evaluate and maintain system efficiency, and may further monitor and record usage, including the disclosure of individual files:

- if it has reason to believe that activities are taking place contrary to this policy, or to OIT policy, or state or federal law or policy
- to respond to an administrative court or judicial court order
- to respond to a request for discovery in the course of litigation
- to respond to a public record request for files which are deemed public records under public records laws

OIT may use information gained in this manner in disciplinary or criminal proceedings. In addition, state or federal law may require disclosure of individual computer files that are deemed public records under public records laws. Communications made by means of OIT computing resources are also generally subject to Oregon's Public Records law to the same extent as they would be if made on paper.

Legal Standards:

All users are expected to abide by all Federal and State laws as outline below. All users of OIT computing resources must comply with all federal, state and other applicable laws; all generally applicable Board of Higher Education and University rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

OIT neither sanctions nor censors individual expression of opinion on its systems. However, the same standards of behavior are expected in the use of electronic mail as in the use of telephones and written and oral communication. Therefore electronic mail, like telephone messages, must be neither obscene nor harassing. Similarly, messages must not misrepresent the identity of the sender and should not be sent as chain letters or broadcast indiscriminately to large numbers of individuals. This prohibition includes unauthorized mass electronic mailings. For example, email on a given topic that is sent to large numbers of recipients should in general be directed only to those who have indicated a willingness to receive such email.

Who May Not Use Computer Facilities

Entry into the computer system, including use of the infrastructure, by individuals not specifically authorized, or attempts to circumvent the protective mechanisms of the systems and files, programs, or any electronic information, is prohibited and may result in disciplinary, criminal or civil sanctions. Deliberate attempts to degrade system performance or capability, or attempts to damage systems, software, or intellectual property of others are strictly prohibited.

___

Prohibited Uses

It is prohibited to use OIT's computing resources in ways that:

1. infringe on another individual's right to privacy or otherwise adversely affect members of the user community;
2. are inconsistent with the academic mission and not-for-profit status of the university violate usage restrictions required by OIT's software, hardware, ISP, or other technology licenses;
3. violate university policies or local, state, or federal statutes
4. allow unauthorized access to someone else's account, use of someone else's username and password, or unauthorized access of remote computers via OIT's network facilities;
5. enable unauthorized reading, copying, deleting, or modification of someone else's electronic materials including email;
6. cause intentional damage to hardware, software, network equipment, security devices, or other technology resources;
7. intentionally create or distribute viruses, worms or other forms of electronic malware;
8. abuse printing privileges, such as printing under a false or someone else's username;
9. send obscene, abusive, harassing, or threatening messages;
10. excessively use network bandwidth or CPU cycles;
11. allow unauthorized use, duplication, or sharing, of copyrighted materials, such as music, images, text, multimedia, commercial software;
12. are for profit-making activities, such as development and sale of software or digital materials, unauthorized work undertaken to support a for-profit company, or other contract work unrelated to OIT's academic mission;

Email and communications prohibited uses

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding chain letters or other pyramid schemes of any type.
6. Use of unsolicited email originating from within the department or network
7. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

Confidential Data

OIT faculty, staff, and student users have varying access to electronic information that is sensitive and confidential. OIT considers the protection of such information and its electronic infrastructure from

unauthorized use to be a key responsibility of all faculty, staff, and student users. Failure to act in accordance with university guidelines may result in disciplinary and/or legal action.

- By law, certain institutional data may not be released without proper authorization. You must adhere to all applicable federal and state laws concerning storage, retention, use, release, and destruction of data. Users are encouraged to seek guidance from an appropriate supervisor, senior officer, or the chief information officer if it is unclear whether or not specific information is confidential.

- You are responsible for the security, privacy, and control of data in your care, access privileges entrusted to you, and your username/password. You must take every reasonable precaution to prevent unauthorized access to confidential data.

- Users must understand the definition of confidential information in the context of your job responsibilities and take steps to ensure that co-workers, staff, and student users understand existing statutes and policies (such as FERPA, HIPAA, Donor Bill of Rights, Digital Millennium Copyright Act, ., and University departmental guidelines that may supplement this agreement). Before granting access to confidential information you should be satisfied that a "need to know" is clearly demonstrated.

- Confidential or otherwise sensitive OIT information must not be stored, shared, or otherwise processed by a cloud computing service, unless the service enters into a legally binding agreement with OIT to protect and manage the data according to standards and procedures acceptable to the university.

Illegal Copying of Software and Other Copyrighted Materials

Copyright infringement and unauthorized access to digital materials may be grounds for legal action. OIT prohibits the illegal use of copyrighted materials as stated in the Digital Millennium Copyright Act (DMCA) http://www.oit.edu/its/dmca. OIT is committed to respond to lawful requests for information. OIT will not protect or defend a user against criminal investigations or lawsuits resulting from intentional copyright infringement.
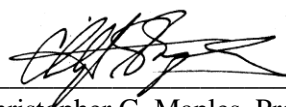
Failure to Comply and Discipline

Faculty and staff users found to have violated this policy may be subject to disciplinary action for cause, up to and including termination of employment. Additional civil and/or criminal actions may be taken by governmental, law enforcement or private entities.

A student accused of violating this policy will be referred to the Dean of Students for action under the Student Code of Conduct, which may result in sanctions that include suspension or expulsion from OIT.

Recommended by:

President's Council- 4/05/11

Approved: _____

        Christopher G. Maples, President

Date:_____June 22, 2011_____