DRAFT – NOT OFFICIAL UNIVERSITY POLICY

University Policy 08-005

Acceptable Use of Computing Resources

Responsible Executive: Chief Information Officer, Vice Provost for University Information Technology

Responsible Office: Office of Information Technology

Effective: July 19, 2016

Last Revised: July 19, 2016

1. Policy Statement

1.1. Oregon State University (university) is committed to a respectful, safe, and ethical environment. This policy defines the expectations for using the university's computing resources.

2. Reason for Policy

2.1. This policy establishes responsibilities associated with the use of university computing resources, including but not limited to facilities, devices, applications, systems, and infrastructure, whether located on university property or used or accessed remotely.

2.2. Additionally, the University Code of Ethics and Code of Student Conduct extend into virtual environments.

3. Scope & Audience

3.1. This policy applies to all university employees, students, contractors, volunteers, visitors, or anyone using university computing resources.

4. Definitions

4.1. **Computing Resources.** The network and communications infrastructure, facilities, devices, applications, and systems owned or provided by the university.

5. Responsibilities & Procedures

5.1. **Acceptable Use of University Computing Resources**

5.1.1. Computing resources are the property of the university and must be used primarily for official university instructional, research, administrative, public service, outreach, and contract purposes.

5.1.2. Minimal personal use of computing resources may be permitted if the use is legal; there is little or no cost to the university; any use is brief; any use occurs infrequently; the use does not interfere with the performance of any university employee's official duties; and the use does not compromise the security, integrity, or access of university computing resources, property, or information.

5.1.3. All users of university computing resources must:

a. Use only those computing resources they are authorized to use and use them only in the manner and to the extent authorized.

b. Keep account credentials, including passwords, confidential. Accounts and credentials must not be shared with or used by persons other than the individual(s) to whom they have been assigned by the university.

c. Not view, use or monitor another person's computer files, programs, accounts, or data without permission, authorization or business need to know.

d. Not circumvent or attempt to circumvent the security mechanisms of any computing resources, without university prior authorization.

e. Not degrade computing resources performance or attempt to degrade or damage computing resources.

f. Not enable settings that automatically forward university e-mail to non-university email addresses.

g. Comply with applicable international, federal, state and local laws, including federal copyright laws; applicable university rules and policies, including the code of ethics and code of conduct; and applicable contracts and licenses.

5.1.4. Personal devices may be used by university community members to access teaching, learning and other resources. Personal devices, unless they use an approved service defined by the Office of Information Security, must not access confidential information.

5.1.5. Individuals using a personal device to conduct university business on behalf of the university shall provide the university access to data on that device that constitutes university business. There are both legal obligations and University policies that may extend to this data.

5.2. **Privacy**

5.2.1. Users have no expectation of privacy regarding any data residing on computing resources. The university may access and monitor its computing resources for any purpose consistent with the university's duties or mission without notice. However, it is the practice of the university to refrain from monitoring individual usage of computing resources unless there is an official, legal or business-related reason to do so.

5.2.2. The university reserves the right to monitor and record the usage of university computing resources by individuals for the following reasons:

a. To evaluate and maintain system efficiency and security;

b. There is reason to believe that activities are taking place in violation of this or other university policy, or local, state, federal, or international law;

c. To respond to a court order or subpoena, to assist law enforcement, or in response to a request from a regulatory oversight entity;

d. To respond to a request for discovery in the course of litigation;

e. To respond to a public record request;

f. For other official university business reason.

5.3. **Enforcement**

5.3.1. Violations of this policy may result in:

a. Removal of content;

b. Denial of access to computing resources;

c. Disciplinary actions up to and including termination or expulsion;

d. Criminal or civil actions, or both;

e. Referral to appropriate law enforcement agencies.

5.3.2. The university may immediately suspend or block access to computing resources to protect the confidentiality, integrity and availability of university or other computing resources or to protect the university from liability.

5.4. **Exceptions**

5.4.1. Exceptions to this policy must be approved by the Vice Provost for University Information Technology, Chief Information Officer.

6. Forms & Tools

6.1. None.

7. Frequently Asked Questions

7.1. None.

8. Related Information

8.1. University Policy 08-015 *University Data Management, Classification, and Incident Response*: https://policy.oregonstate.edu/UPSM/08-015_university_data_management_policy.

8.2. Code of Student Conduct: https://studentlife.oregonstate.edu/sites/studentlife.oregonstate.edu/files/student-conduct-community-standards/Code/code_of_conduct_83-2_compressed.pdf.

8.3. University Code of Ethics: https://leadership.oregonstate.edu/sites/leadership.oregonstate.edu/files/190118_adopted_university_code_of_ethics.pdf.

8.4. The Information Security Advisory Committee is a committee charged with reviewing and recommending information technology (IT) security policy. The committee is appointed by the Chief Information Officer and Vice President for University Information Technology. For more information, visit the university's IT website at https://uit.oregonstate.edu/governance.

9. History

9.1. Adopted: Oregon State University adopted University Policy 08-005 *Acceptable Use of Computing Resources* on July 19, 2016.

9.2. Revised: University Policy 08-005 *Acceptable Use of Computing Resources* was revised on XXX, 2022.

9.3. Next scheduled review: Month, year

10. Website

10.1. University Policy Office will insert the web address to the location of this policy in the University Policy & Standards Manual.

11. Contacts

Department	Phone Number	Website
Office of Information Security	541-713-3363	https://uit.oregonstate.edu/infosec