

Policy Title: Acceptable Use of University Computing Resources			
Policy #:	FA-UCS-003		
Responsible Office:	University Computing Services		
Responsible Administrator:	Vice President for Finance and Administration		
Date Reviewed:	September 2014		Revisions Made? Yes ___ No <u>X</u>
Date of Next Review:	September 2019		

PURPOSE

The intent of this document is to promote the responsible use of computing resources.

The university encourages the sharing of information and free expression of ideas. Information and infrastructure are provided to further this purpose. There is an obligation on the part of those using these facilities and services to respect the intellectual and access rights of others--locally, nationally and internationally.

AUDIENCE

All users of WOU computing and network resources.

DEFINITIONS

N/A

POLICY STATEMENT

WOU requires professional behavior and acceptable use of computing resources.

PROCEDURES

Be knowledgeable about laws and policies

Your use of WOU computing and networking resources is governed by:

- *Extensive federal and state law and policy*
- *Internet acceptable use practices*
- *WOU policy or contractual commitments*
- *WOU Technology policy*

All WOU policies regarding the appropriate use of University resources, responsibility for University institutional data, and personal conduct apply to your use of WOU computing and networking resources. In addition, your use of WOU resources must comply with the restrictions and acceptable practices established specifically for these resources and these data. Faculty and staff use of these systems is subject to Oregon State law for employees of state agencies. See additional information section below, which lists applicable laws, policies and WOU resources to help you understand the University's and your obligations.

You should be aware that law and policy relating to the use of state resources specifically prohibit faculty and staff from:

- Using WOU computers, networks, or other computing services for personal gain. For example, it would be improper to use your account to promote your outside business, to display commercial advertising, or to perform work for profit in a manner not authorized by the University.*
- Using WOU resources for partisan political purposes, such as using email to circulate advertising for political candidates or to help defeat a ballot measure.*

Evidence of illegal activities or policy violations will be turned over to the appropriate authorities as soon as possible after detection. Depending upon their nature, violations of law or policy will be met with responses including revocation of access, suspension of accounts, disciplinary actions, and prosecution.

***Protecting
WOU's
infrastructure***

As the computing and networking infrastructure of the WOU underlies many crucial activities for the entire University community, WOU must protect and sustain the operation of those facilities.

As such, WOU will take all legally allowed steps it deems appropriate to remedy or prevent activities that, in WOU's judgment, endanger the orderly operation of WOU's networks or systems, and/or that threaten WOU's network connections to the Internet and/or other institutions or networks.

The University reserves the right to deactivate a Web page at any time and without notice for violations of policy or for security reasons.

***WOU Residence
Halls***

Computing and networking services in WOU Residence Halls are provided to support student academic activity. If you are living in WOU residence halls, please take the time to familiarize yourself with the [rules for using those services](#).

Protect your passwords

Choose your passwords carefully, change them regularly, and protect them from abuse.

Your Pawprint credentials gives you access to many WOU services. You are responsible for any use of your Pawprint credentials. You may not share your personal Pawprint credentials.

Know your responsibilities

In the course of using WOU services, you may store and/or transmit data that come from institutional sources. Some data is more sensitive than other. You are responsible for knowing the applicable [data security standards and policies](#), appropriate places to store the data, and controlling who can access the data.

Employees of the University are responsible for protecting institutional data, such as student records, protected health information, and personally identifiable information. Where and how confidential and restricted data is stored matters; for example, if confidential data is stored on a portable device it must be suitably protected.

Monitoring and privacy

WOU is committed to safeguarding the privacy of personally identifiable information, including personal financial information, educational records, and health records. For employees, be aware that all email and other electronic information pertaining to WOU business is "owned" by the university, regardless of where it is kept.

WOU may monitor user activities and access any files or information in the course of performing normal system and network maintenance while investigating policy or violations.

University policies and procedures are consistent with overall state, federal, and institutional policies regarding release of student and employee information as outlined in the Oregon Public Records Law, ORS 192.501 - 192.505; Oregon Faculty Records Law, ORS 351.065; the Oregon Student Records Law, ORS 351.070(2)(e); the Federal

Educational Rights and Privacy Act of 1974; the WOU Faculty Handbook; and the WOU Acceptable Use of Computing Resources Policy.

- Data which is identifiable to particular individuals (e.g., inclusion of names, social security numbers, addresses, telephone numbers), shall be used only within the scope of an individual's responsibilities, e.g., instructors may access data for classes which they teach, departments for their majors, etc.
- Information extracted and used to conduct the user's duties shall be considered unofficial data and shall not be used for publication.
- Data analysis of units or groups within the institution, or with organizations external to the University, should be coordinated with the appropriate central

administrative office.

- Data that is saved locally must be adequately protected from outside access.
- Saved data must be updated frequently enough that the likelihood of incorrect data being used is minimized.
- Anyone with information system access must ensure that such data is not available to individuals who do not have access to it, or who do not have a legitimate "need to know." An individual with information system access is responsible for the security of his/her access.
- Information extracted from the information system and used to complete survey documents or to be distributed to any publication having general readership, or if the information might otherwise have an impact on the external image of WOU, must be presented for review and approval by the appropriate central administration office.
- Requests for data or the use thereof which are outside the user's responsibilities must be authorized in advance by the appropriate central administrative office, consistent with a written request stating the use of the data.
- Requests for release of any individual or aggregate student or employee information to anyone outside of WOU who has a legitimate "need to know" must be authorized in advance by the appropriate central administrative office consistent with a written request stating the use of the data.
- Subpoenas for individual or aggregate student or employee information or any request from law enforcement authorities (including campus security, OSP, FBI, CIA, District Attorney) should be referred to the appropriate central administrative office.

Records management and release of information

Except as noted by an agreement, a law, or a University policy (such as copyright policy), WOU owns all data and records, and all associated copyrights created by WOU employees within the course of employment. All information (including email) relating to University business should be maintained in accordance with records retention policy and procedures. This applies to email and other electronic records, regardless of where the records are stored, including on personally-owned computers, "cloud" or externally provided services, personal email services and/or other non-WOU computers.

Email use

Email services at WOU are provided to support you in your work and education, as well as to support communication from WOU administration. Your use of email services at WOU should respect others and must not interfere with the operation of WOU computers and networks.

Employees may use such resources for employment related communications, including related communications, subject to the provisions of any applicable collective bargaining agreement.

WOU administrative email messages will be sent to faculty, staff, students,

and affiliates of WOU at their official WOU email address.

External Email and Cloud Service Providers: *Email is inherently insecure. Sending confidential or restricted information (such as protected health information or FERPA information) by email is unsafe, especially if you forward WOU email off-campus to an external email service provider. External email service providers typically do not provide legal protection or accountability for official WOU records and information and do not comply with federal, state and WOU regulations. However, the University has [encryption services available](#). WOU employees should not forward their WOU email to a non-WOU email address, since doing so may put you and WOU at risk of violating regulations such as FERPA, HIPAA.*

Obscene materials and pornography

University employees may not use WOU information technology resources to view, store or access obscene materials, such as pornography, except when clearly required to do so in the course of their work.

Copyright laws apply to you

You may not copy or use any software, images, music, or other intellectual property (such as books or videos) unless you have the legal right to do so.

Educational institutions are not exempt from the laws covering copyrights. Most software, images, music, and files available for use on computers at the WOU are protected by federal copyright laws. In addition, software, images, music, and files normally are protected by a license agreement between the purchaser and the software seller. It is WOU policy to respect federal copyright and license protections.

- *Software and information resources provided through the University for use by students, faculty, and staff may be used on computing equipment only as specified in the various software licenses. It is against University policy for you to copy or reproduce any licensed software on University computing equipment, except as expressly permitted by the software license.*
- *It is a serious violation of WOU policy to make or use unauthorized copies of software on University-owned computers or on personal computers housed in University facilities.*

Unauthorized use of software, images, music, or files is regarded as a serious matter and any such use is without the consent of WOU. If abuse of computer software, images, music, or files occurs, those responsible for such abuse will be held accountable.

More about copyrights

- [WOU File sharing information](#)
- [WOU HEOA \(higher education opportunity act\) Plan](#)

FORMS

N/A

AUTHORITY

Name & URL of authority:

Oregon Administrative Rule 574-031 (Code of Student Responsibility), specifically OAR 574-031-0030 (http://arcweb.sos.state.or.us/pages/rules/oars_500/oar_574/574_031.html)

RESPONSIBILITY

University Computing Resources is responsible for this policy and may be contacted at 503-838-8925 or ucshelpdesk@wou.edu.

Individuals are personally responsible for on-line statements. Violations of computing acceptable use policies that constitute a breach of the Code of Student Responsibility, Faculty Handbook, or other appropriate and pertinent WOU rules and regulations will be referred to appropriate authorities. University personnel may take immediate action as needed to abate ongoing interference with network and system operations or to ensure system integrity.

Alternate formats of this policy may be requested from the Office of Human Resources.