

OLYMPIC COLLEGE POLICY

TITLE: Acceptable Use Policy

POLICY NUMBER: OCP 200 - 17

REFERENCE: RCW 42.52.160, RCW 42.52.180, RCW 42.17, WAC 292-110-010,
<http://isb.wa.gov/policies/security.aspx>,
<http://www.governor.wa.gov/execorders/archive.asp>, <http://ethics.wa.gov/>

I. Purpose

This policy is intended to provide campus users with guidelines for responsible and appropriate use of the campus computing and technology resources. Olympic College (OC) owns all college computing systems and applications and reserves the right to determine at any time what constitutes appropriate use of the College network. Resources are provided to support the mission of Olympic College including educational, research and administrative functions. The role of OC information technology is to foster and support the learning processes, provide services for students, faculty and staff, and facilitate connectivity between college sites, the community, on-line learning resources, and other educational institutions. The Acceptable Use Policy and Procedures are designed to provide a framework to assure that the technology used at Olympic College is used within the Washington State Department of Information Services (DIS) Information Technology (IT) Security Audit Process and to identify the appropriate uses of technology. The policy outlines prohibited uses and identifies actions that can have a negative service impact on all users.

It is not the intent of this policy to expand, diminish or alter Academic Freedom, but to provide an appropriate framework for the proper exercise of those freedoms consistent with Washington State laws and the Academic Freedom provision in the Olympic College collective bargaining agreement with the OC Association for Higher Education.

This policy applies to all OC employees, students and/or non-employees who may be authorized to use any OC technology resources and applies to the use of state resources at OC facilities or any use of OC technology resources, regardless of its location.

OLYMPIC COLLEGE POLICY

II. Definitions

- A. **Information Technology Resources (ITRs):** All electronic hardware, software and associated data, goods, equipment and services that support or include the following: administrative/management information systems; desktop computing; library electronic resources; multi-media, data, video and voice networks; telephone systems and telecommunications; voice mail; automated data processing, databases, electronic mail (E-mail); Internet access; scanners; electronic publications, including video; or any similar electronic based medium.
- B. **User:** Any individual authorized to use one or more ITRs to include Olympic College employees, students, student employees (including a District officer), contractor, visitor, volunteer, community member or any other person who uses the college's electronic information resources.
- C. **Authorized Account:** A user account established by College staff with appropriate password protection that authorizes use of College ITRs.

III. Use of OC Network

- A. **Acceptable Use.**
 - 1. Olympic College's ITRs are to be used for legitimate college business, and for facilitating the exchange of information to further the college's educational, research, administrative and community service mission. Such uses shall at all times be consistent with state law and the conduct of official College duties.
 - 2. Employees and students may use OC computer, programs and data to which each individual has authorized access including using OC networking, access to the Internet, and use of computing and networking facilities.
 - 3. Use of ITRs that may be reasonably related to the conduct of official state duties may include:
 - i. Notice of public interest and public service events pertinent to the mission of the college, such as lectures, or authorized combined fund drive, etc.
 - ii. Notice of campus events and gatherings such as opening days, concerts, etc.

OLYMPIC COLLEGE POLICY

- iii. College-wide notifications which are used for connecting employees, programs and community (e.g., press releases, announcements, or schedule changes).
- iv. Inclusion of an incidental message - such as "happy birthday" - in an e-mail message that was otherwise sent for an official business purpose.

4. **Permitted De Minimis Staff and Faculty Personal Use Under Limited Circumstances:** De Minimis use standards will not apply to students. Users may not make use of the college's ITRs, such as to access networks, databases, e-mail, electronic bulletin boards, or the internet, for purposes that are personal to the user and/or unrelated to the missions of the college. However, a very limited personal use of College ITR resources that supports organizational effectiveness and does not undermine public trust and confidence may be allowed **only** if each of the following conditions are met: (a) There is little or no cost to the state; (b) Any use is brief in duration, occurs infrequently, and is the most effective use of time or resources; (c) the use does not interfere with the performance of the officer's or employee's official duties; (d) the use does not disrupt or distract from the conduct of state business due to volume or frequency; (e) the use does not disrupt other state employees and does not obligate them to make a personal use of state resources; and (f) the use does not compromise the security or integrity of state property, information or software.

De Minimis use of state computers and other equipment to access computer networks or other data bases are permitted only when such use conforms to ethical standards in this section and the use is not otherwise prohibited under WAC 292-110-010 and RCW 42.52. De minimis use does not apply to any use of ITR resources that violates any federal, state, or local laws or college policies including, but not limited to, use of such resources for discriminatory, harassing or retaliatory purposes. Examples of de minimis personal use of technology resources may be found at www.ethics.wa.gov/RESOURCES/FAQ.htm.

OLYMPIC COLLEGE POLICY

B. Prohibited Use

1. In accordance with the Washington State Constitution, State and Federal laws, RCW 42.52.160 and WAC 292-110-010(6), the following private activity using state resources is explicitly prohibited at all times:
 - i. Any use for the purpose of conducting an outside business or private employment;
 - ii. Any use for the purpose of supporting, promoting the interests of, or soliciting for an outside organization or group, including, but not limited to: a private business, a nonprofit organization or a political party (unless provided for by law or authorized by an agency head or designee);
 - iii. Any use for the purpose of assisting a campaign for election of a person to an office or for the promotion of or opposition to a ballot proposition;
 - iv. Any use for the purpose of participating in or assisting in an effort to lobby the state legislature, or a state agency head;
 - v. Any use related to conduct that is prohibited by federal or state law or rule, or a state agency policy; and
 - vi. Any private use of any state property that has been removed from state facilities or other official duty stations, even if there is no cost to the state. Rules and examples can be viewed at www.ethics.wa.gov/RESOURCES/FAQ.htm. Employees may also test their understanding of ethics laws at the same site.

Examples of prohibited use would include the use of ITRs for running a personal business, entertainment, on-line gaming, political or religious purposes, etc.

2. Based on state ethics standards and protection for the campus use of internet radio for non-instructional use, turning off the proxy server and other such activities are not permitted.

C. User Responsibilities

All users of the College's ITRs are advised that there is no legitimate expectation of privacy. The College reserves the right to monitor an individual's use of its systems and technology resources. Records may be

OLYMPIC COLLEGE POLICY

subject to disclosure under the public disclosure law or may be disclosed for audit or legitimate state operational or management purposes.

1. College ITRs shall be used in compliance with this Acceptable Use Policy, with all collective bargaining agreements, College policies and regulations and with local, state and federal laws and regulations.
2. Users shall not share their authorized accounts or account passwords with others.
3. Users shall not delete, remove or modify in any manner the required password protection on Users account.
4. Users shall report to an appropriate administrator suspected misuse of their account.
5. Users shall respect the privacy of others by not (without proper administration authorization) inspecting, using, broadcasting, or modifying ITRs assigned to other users.
6. Users shall not interfere with the performance of any ITR, or block access to any ITR.
7. Activity that promotes excessive bandwidth or impairs the function of the College's network for instruction and College business is not permitted.
8. In the event that the function of the College network is being impaired by activities that promote excessive bandwidth, the IT department will identify, categorize, and prioritize activities. Unauthorized activities will be terminated. If necessary to restore the functionality of the network, the IT department reserves the right to modify temporarily the bandwidth of some legitimate uses on the network. In general, the key functions of the College (determined by IT/President/other?) and any instruction by faculty that involves direct contact with students will have priority, followed by instructional activities by faculty that involve research or class preparation.
9. Users shall not load or use any software not approved by the Information Technology department, unless modified by a memorandum of understanding. Unapproved software may promote unrestricted file sharing to campus and internet users which often disrupts network transmissions and does not allow appropriate security and copyright protections to be maintained.

OLYMPIC COLLEGE POLICY

- a) No user shall introduce invasive computer software such as viruses into any ITR.
- b) All ITR users are required to utilize all anti-virus software provided by the college to protect electronic information.
- c) All use of data and software on college ITRs must comply with related licensing agreements and with copyright laws. Users are not authorized to install software or modify the configurations of ITRs unless there is an established memorandum of understanding with the College IT department that outlines the roles and responsibility of the authorization.
- d) User shall not modify any ITR to prohibit or circumvent network monitoring, logging, or retention of workstation log files.
- e) Users shall be responsible for information they transmit through the College's ITRs and shall comply with the acceptable use policies of the Internet and all local, state and federal laws and regulations.
- f) Users shall not conceal or falsify their identity (spoofing, masquerading, using anonymous mailers/mail relays, providing false identifications, etc.) or modify a system configuration to conceal their activity when using the College's ITRs.
- g) ITRs of the College shall not be used to access, transmit or store information that constitutes or promotes the following, except as such access relates to the academic freedom of a College faculty member or student research for a class:
 - 1) Discrimination on the basis of race, creed, color, age, sex or gender, religion, disability, or sexual orientation
 - 2) Sexually explicit materials
 - 3) Sexual harassment
 - 4) Content that promotes violence or hate crimes

OLYMPIC COLLEGE POLICY

- h) The following ITR activities are illegal under federal and/or state statute(s), and are therefore prohibited at Olympic College:
 - 1) Copyright infringement
 - 2) Promotion of or opposition of any political candidate or ballot proposition, in violation of RCW 42.52.180
 - 3) Solicitation of political financial contributions
 - 4) Personal business interests, or
 - 5) Any other unlawful activity.
 - i) To protect instructional bandwidth and College business functions, the College reserves the right to block College ITRs' access to sites (e.g. malware, virus) and content not in compliance with this policy or that may harm essential College functions.
 - j) No user shall transmit unsolicited and unwanted or threatening messages to any recipient. Examples of such inappropriate transmissions include, but are not limited to, phone calls, faxes or e-mails that are both unsolicited and unwanted, e-mail mass mailing (spamming), and the transmission of invasive computer software.
10. Devices of any nature may not be connected to the network without prior approval of the IT department. Any user connecting (wired or wireless) personally owned information technology equipment is subject to all College policies and procedures. In addition to prior approval, all personally owned ITRs shall:
- i. have current anti-virus software, and application / operating systems security patches installed prior to connecting to College networks; and
 - ii. The capability to control or modify network settings must be approved and configured by the IT department.

IV. Violations and Monitoring

- A. Violation of the Acceptable Use Policy may result in the temporary or permanent denial of access to Olympic College's ITRs, and the imposition of civil or criminal sanctions by appropriate authorities including but not

OLYMPIC COLLEGE POLICY

limited to federal, state, or local agencies. Appropriate disciplinary action may also be taken by the offices of the Vice President for Instruction, the Vice President of Student Services, the President, or the Board of Trustees.

- B. Users are advised that if monitoring of user activities reveals possible evidence of violation of any college policy or procedure or any other applicable law or regulation, Olympic College may use or provide such evidence for use in appropriate investigations which could result in discipline or other sanctions. OC may permit the inspection, monitoring, or disclosure of ITRs:
1. When required or permitted by law, including public records law, or by subpoena or court order
 2. When OC or its designated agent reasonably believes that a violation of law or policy has occurred or
 3. When necessary to monitor and preserve the functioning and integrity of OC ITRs or related computer systems or facilities.

V. Privacy and Access

- B. The College cannot assure that messages sent through ITRs are private or secure, although the College will make reasonable efforts to maintain the confidentiality of communications, consistent with Washington law. Authorized personnel shall have access to data under users' control. Electronic messages ordinarily will be backed up and retained under retention schedules approved by the appropriate records committee in accordance with state law. Users should assume that all electronic messages may be stored for a defined period of time.
- C. Users of college electronic information resources must not intentionally seek information about, browse, obtain or retain copies of, or modify personal or private files, records, messages, or passwords belonging to other people, whether at any of the facilities of Olympic College or elsewhere, unless specifically authorized in advance to do so by those individuals. Users should assume, however, that their own files, records, messages or use/audit logs may be seen by others, including:
1. IT support staff in the course of system or network administration, maintenance, and service duties,

OLYMPIC COLLEGE POLICY

2. Authorized appropriate administrator in accordance with IT policies, or
 3. When recipients or others choose to forward or disclose items they have been sent.
- D. Files, records, messages, and passwords also may be disclosed when required by law. Electronic messages created or placed on the college's ITRs may be considered writings, and all writings are public records subject to disclosure to any requester in accordance with Washington's Public Disclosure Act, chapter 42.17 RCW. Electronic messages also may be legally required to be disclosed to third parties in other circumstances, such as in discovery conducted during litigation. Investigations, including investigations into suspected illegal acts or violation of College policy may occur with or without notification to the employee.

Recommended by

*Submitted to President's Cabinet for
Review*

Approved by President

Submitted to Board of Trustees

Approved by Board of Trustees

Published in Washington

Administrative Code

Barbara Martin, Vice President for Administrative Services

November 24, 2009

November 24, 2009

February 23, 2010

February 23, 2010

n/a