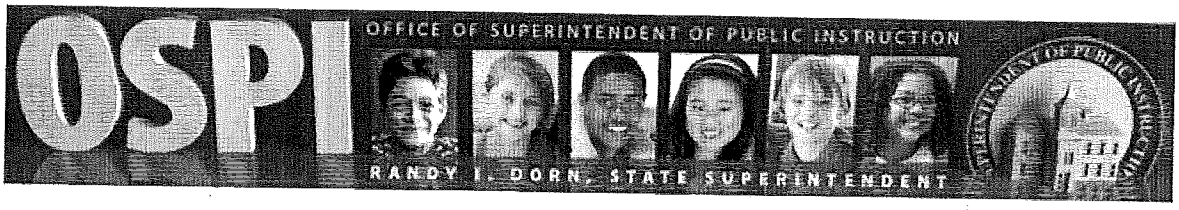

TITLE:	COMPUTER SYSTEM ACCEPTABLE USE POLICY
APPLIES TO:	ALL PERSONS ACCESSING OSPI SYSTEMS ON SITE AND/OR REMOTELY
LAWS/WACS:	Ethics in Public Service Act: RCW 42.52, RCW 42.56 and WAC 292-110-010
NOTE:	*Replaces Electronic E-mail Usage and Retention Policy and the Network and Internet Acceptable Use Policy*
EFFECTIVE DATE:	March 1, 2009, Revised February 18, 2011
APPROVAL:	Randy I. Dorn, State Superintendent

1.0 Why is a Computer System Acceptable Use Policy needed?

OSPI is committed to protecting OSPI's employees, partners and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a collaborative effort involving the participation and support of every OSPI employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable and legitimate use of computer equipment at OSPI. These rules are in place to protect both the employee and the agency. Inappropriate use exposes OSPI to risks including virus attacks, compromise of network systems and services, ethical, and legal issues.

2.0 Who does the policy apply to?

This policy applies to employees, contractors, consultants, temporaries, co-op students, and other workers accessing OSPI systems on-site or remotely.

APPROVED
Executive Ethics Board
Date 9-9-11

3.0 What systems does this policy apply to?

This policy applies to all systems and equipment that are owned or leased by OSPI. All OSPI maintained systems are the property of OSPI, including but not limited to computer hardware, software, operating systems, file transfer systems, networks, and all network user accounts providing access to document storage systems, electronic mail, and the Internet.

Postings by employees to on-line discussion groups, social networking sites, blogs, or bulletin boards from OSPI equipment using OSPI login names or e-mail addresses are also covered by the General Use and Ownership conditions and standards as well as the prohibited uses outlined in this policy.

4.0 What are my responsibilities and what do I have to know and do?

4.1 General Use and Ownership

1. OSPI systems are to be used in support of education, be consistent with the mission of OSPI, and are related to official state business. OSPI management will ensure that all employees, business partners, and contractors accessing OSPI systems receive an orientation on the systems and the appropriate use of state resources. All persons requiring access to OSPI hardware, software, networks, and other electronic resources are required to complete annual security training offered by the agency.
    a. While OSPI provides a reasonable level of privacy, users should be aware that the data and system logs they create on agency systems remain the property of OSPI. Examples of this data include, but are not limited to: Internet history, file access, and e-mail.
2. Washington Administrative Code (WAC) 292-110-010, Use of State Resources, states that agency employees may make an occasional but limited personal use of e-mail or the Internet only if each of the following conditions and standards 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 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;
    f. The use does not compromise the security or integrity of state property, information, or software.
3. Only OSPI Information Technology (IT) staff are authorized to install software on or modify OSPI owned hardware.
4. No software not owned or obtained by OSPI may be loaded onto OSPI owned equipment.
5. No hardware not owned or obtained by OSPI may be connected to the OSPI network. Examples include but are not limited to: laptops, smartphones, monitors, USB memory, cameras, music players, printers, and storage devices.
6. For security and network maintenance purposes, OSPI IT staff may monitor equipment, systems, Internet use, and network traffic at any time.

APPROVED
Executive Ethics Board
Date: 9-9-11

7. OSPI will audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level and user level passwords should be changed quarterly.
2. All PCs, laptops workstations, and smartphones must be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less, or by logging-off when the computer will be unattended.
3. All computers connected to the OSPI Internet, intranet, or extranet shall be continually executing approved virus-scanning software with a current virus database.
4. Employees should use caution when opening e-mail attachments received from unknown senders, especially if an e-mail is automatically placed in a Junk or Spam e-mail folder. These e-mails and their attachments may contain viruses, e-mail exploits, or Trojan horse code.

4.3. Public Disclosure and Record Retention

Voice mail messages, e-mail messages, instant messages, text messages, and system logs are public records and subject to disclosure in accordance with agency policy and public records laws in Chapter 42.56 RCW and WAC 392-105.

Documents, spreadsheets, e-mails and other electronic content must be retained in accordance with state retention schedules. Refer to the Record Management policy for direction.

4.4. Unacceptable use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a computer if that computer is disrupting production services).

Under no circumstances is an employee of OSPI authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing OSPI owned resources.

The listed items below are by no means exhaustive, but provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Using an OSPI computing asset to actively engage in procuring or transmitting material that is in violation of harassment, pornography, sexual harassment, discrimination or hostile workplace policies and laws.
2. Promoting political or religious beliefs.

APPROVED
Executive Ethics Board
Date: 9-9-11

3. Using OSPI systems for personal gain not related to OSPI business activities or to conduct an outside business or other employment.
4. Violations of the rights of any person or agency protected by copyright, trade secret, trademark, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by OSPI.
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Effecting security breaches or disruptions of network communication with malicious intent. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
7. Executing any form of network monitoring which will intercept data not intended for the employee's system, unless this activity is a part of the employee's normal job/duty.
8. Circumventing user authentication or security of any system, network or account.
9. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's, via any means, locally or via the Internet, intranet or extranet.
10. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
11. Unauthorized use, or forging, of e-mail header information.
12. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
13. Forwarding unsolicited e-mails from within OSPI's networks of other Internet, intranet or extranet service providers on behalf of, or to advertise, any service hosted by OSPI or connected via OSPI's network.

5.0 What are the consequences for not following the policy?

All employees are required to sign a statement (attached) acknowledging the agency's policy and standards regarding the acceptable use of e-mail, the Internet and other OSPI systems.

OSPI may discontinue system access to OSPI systems during an investigation. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPROVED
Executive Ethics Board
Date: 9-9-11

COMPUTER SYSTEM ACCEPTABLE USE POLICY

I have received and read the Computer System Acceptable Use Policy and understand that this will be placed in my state personnel file located in the OSPI Human Resources Office.

Printed Name:_____

Signature:_____

Date: _____

Please return this form to the OSPI Human Resources Office after signing. If you have any questions you may contact the HR office at (360) 725-6270 or HRoffice@k12.wa.us.

APPROVED
Executive Ethics Board
Date: 9-9-11