AGENCY POLICY

Office of Superintendent of Public Instruction

POLICY TITLE	**Technology Acceptable Use Policy**		
NUMBER	TE-011	**EFFECTIVE**	
APPLIES TO	All Persons Accessing OSPI Systems On-site and/or Remotely	**CONTACT**	Chief Information Officer

[Original Effective Date: 3/1/09; Previous revisions: 2/18/11, 2/8/12, 11/16/12, 9/9/13, 12/9/14, 5/8/15, 11/3/15, 6/16/20, 8/5/21]

PURPOSE

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.

This policy outlines the acceptable and legitimate use of computer equipment at OSPI. These standards 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.

SCOPE

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

This policy applies to all systems and equipment that are owned, leased, or used by OSPI. All OSPI maintained systems are the property of OSPI, including but not limited to computer hardware, software, data, networks, user accounts, on-premises or cloud-based storage systems, email, and Agency presence on the Internet.

Employee participation in online discussion groups, social networking sites, collaborative sites, or blogs using OSPI login names or email addresses are also covered by the General Use and Ownership conditions and standards, the prohibited uses outlined in this policy, and the Social Media for Agency Business Policy.

All devices including, but not limited to, PCs, laptops, tablets, workstations and smartphones connected to the OSPI Internet, intranet, or extranet, or receiving OSPI services or data are also

Approved by the Executive Ethics Board
January 13, 2023

covered by the General Use and Ownership conditions and standards and the prohibited uses outlined in this policy.

POLICY

GENERAL USE AND OWNERSHIP

1. OSPI systems and data are to be used in support of OSPI's mission, 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.
    a. ***All persons requiring network accounts are required to complete annual security training offered by the agency. All persons requiring Agency email addresses are required to complete annual security training and email retention training offered by the agency.***
    b. 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 and may be subject to public disclosure requests. Examples of this data include, but are not limited to: Internet history, file access, and email.
2. De Minimis Use: As authorized by Washington Administrative Code (WAC) 292-110-010, Use of State Resources, agency employees may make an occasional but limited personal use of email 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 and occurs infrequently;
    c. The use does not interfere with the performance of the employee's official duties;
    d. The use does not disrupt other state employees and does not obligate them to make a personal use of state resources; and,
    e. The use does not compromise the security or integrity of state property, information, or software.
    f. The use is not for the purpose of conducting an outside business, in furtherance or private employment, or to realize a private financial gain.
    g. The use is not for supporting, promoting the interest of, or soliciting for an outside organization or group.

3. OSPI's Technology Services and Standards Group and Chief Information Officer (CIO) maintain the standards for the acquisition or purchasing of technology products and services

    a. Only OSPI Information Technology (IT) staff are authorized to install software on, or modify, OSPI owned hardware. Examples include, but are not limited to: web-based software, freeware, shareware, trials, and demos, personally owned software or hardware, software or hardware purchased by other agencies, ESD's, or school district's.

    b. Only approved OSPI staff are authorized to agree to software Terms of Service (TOS), or User Agreements (otherwise known as "click through agreements") on behalf of the Agency.

4. Only software or hardware purchased or acquired by OSPI, and approved by the CIO or the Technology Services and Standards Group may be installed onto OSPI owned equipment.

5. Hardware that is not owned or obtained by OSPI may not be connected to the OSPI internal network. Examples include, but are not limited to: laptops, tablets, 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.

7. OSPI Wi-Fi is for business use only, which includes de minimis use as defined above by WAC 292-110-010.

8. MiFi points (also known as hotspots, tethering, personal Wi-Fi, or jetpacks) are not allowed in OSPI buildings. They may be used outside of the agency to access the internet.

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

10. Please report immediately to Human Resources if you are aware of or feel that this policy has been violated.

SECURITY AND PROPRIETARY INFORMATION

1. User Login IDs and passwords are considered confidential data and may not be shared. Authorized users are responsible for the security of their passwords and accounts. There are no valid reasons to share individual passwords. Disclosure of individual passwords constitutes a violation of this policy. System level and user level passwords should be

changed at least quarterly and must be significantly different than the prior four passwords and is enforced by operating system rules.

2. All systems 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 systems must be running approved and up to date virus-scanning software, anti-malware software and have been patched to the current Operating System level for that device.
4. Employees shall use caution when opening email attachments received from unknown senders, especially if an email is automatically placed in a Junk or Spam email folder. These emails and their attachments may contain viruses, email exploits, or Trojan horse code.
5. OSPI Helpdesk must be notified immediately any time a device with access to, or containing OSPI data, is no longer in the possession of OSPI employees.

PUBLIC DISCLOSURE AND RECORD RETENTION

Employees, contractors, and anyone else conducting business on behalf of the agency are responsible for managing all electronic records they create regardless of the platform or system used. All individuals are accountable for:

- Knowing the records retention schedules and managing their records in accordance with Chapter 40.14 RCW and WAC 434.662. Please see the Records Information Management policy for more information on records retention.
- Complying with agency policy and public records laws in Chapter 42.56 RCW and WAC 392-105.
- Thoroughly searching, locating, and providing responsive records to the Public Records Office, upon request. Please see the Records Information Management policy for more information on public records.

UNACCEPTABLE USE

The following activities are, in general, prohibited and are considered security violations. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Unless otherwise noted, all exemptions require prior CIO approval.

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

1. Revealing your account password to others or allowing use of your account by others. This includes supervisors, assistants, co-workers, Helpdesk, and family members.
2. 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.
3. Promoting political or religious beliefs.
4. Using OSPI systems for personal gain not related to OSPI business activities or to conduct an outside business or other employment.
5. 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.
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.
7. Executing any form of network monitoring which will intercept data not intended for the employee's system.
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 account, via any means, locally or via the Internet, intranet or extranet.
10. Sending unsolicited email 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 email header information.
12. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
13. Forwarding unsolicited emails 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.

14. Using non-OSPI email accounts to conduct OSPI business without approval from Executive Services.
15. Using unapproved products that provide remote control of IT services.
16. Storing confidential (category 3 or 4) unencrypted data on USB drives or mobile devices.
17. Using of dial-up services unless there is no other way to satisfy a business need. Dial-up access, if used, must be approved by the CIO or the Technology Services and Standards Group and documented in the Agency IT Security Program.

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.

EMPLOYEE COMPLIANCE WITH THIS POLICY

All employees are required to sign a statement (attached) acknowledging the agency's policy and standards regarding the acceptable use of email, 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.

In conjunction with this policy, please view our Technology Standards page on our intranet to help better understand our agency's technology standards.

LAWS, RULES, OTHER AUTHORITY

Ethics in Public Service Act: RCW 42.52,
RCW 42.56 and WAC 292-110-010
Records Information Management Policy
Telework Policy

APPROVED	
Superintendent's Signature	Date Signed

Approved by the Executive Ethics Board
January 13, 2023