

SUBJECT: Acceptable Use of Computing and Communications Resources

PURPOSE:

This establishes the Employment Security Department's (ESD) policy regarding the use of computing and communications resources. Department computing and communications resources are valuable tools for conducting state business. This policy is not intended to discourage appropriate use of these tools, but to clearly define inappropriate use.

SCOPE:

This policy applies to all ESD employees. The acceptable use of ESD's network resources by partners is described in resource sharing agreements. The acceptable use of ESD's network resources for public users in ESD's resource rooms is displayed on the public use computer systems and/or by posted notifications. The acceptable use of ESD's network resources for contractors and vendors is described in the contracts between ESD and contractor or vendor.

DEFINITIONS:

Blog: A blog (a contraction of the term "web log") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Cloud storage: Data that is saved to an off-site storage system instead of to an ESD hard drive or network server and is maintained by a third party. The [Internet](#) provides the connection between the user's computer and the remote storage.

Computing and communications resources: Technology products and services, including but not limited to, computers, peripherals, fax machines, electronic messaging systems, state controlled networks, servers, telecommunications systems, wireless communications devices (such as cell phones, "WiFi", Bluetooth), and ESD provided internet access.

Confidential information: Information that is protected by state or federal laws, including, without limitation, information about unemployment insurance claimants, employers, WorkSource clients, employees, vendors or contractors, and agency systems.

Content filter: A department managed tool that controls material delivered from the World Wide Web and determines what will be available to department web users.

Department: The Employment Security Department.

Division designee: One or more individuals (e.g., system administrator, administrative assistant, etc.) appointed by a division's assistant commissioner or director to ensure compliance with this policy.

Electronic messaging system: Any electronic messaging system that transmits and/or stores voice recordings or typed communication. These messaging systems are commonly referred to as voice mail, email, and text messaging.

Encryption: The translation of data to make it unreadable except to those in possession of a secret key, cipher, or password.

Firewall: A system or combination of systems and software that enforces access control policies between two or more networks.

Hoaxes, hypes, chain letters and spamming: Terms used to describe electronic messaging that is sent to a large number of recipients or is intended to eventually spread to a large number of recipients. The content of these messages does not pertain to official state work.

Instant messaging: A type of communications service that enables a person to engage in instantaneous direct person to person communication with another individual or individuals. Instant messaging includes, but is not limited to, internet based chat and online messaging services such as Google Talk.

Malware: Short for malicious software, software designed specifically to damage, disrupt or cause a system to perform in a way other than its designed purpose, such as a virus, worm, spyware or Trojan horse.

Network: An interconnected group of computers which allow users to share resources and communicate.

Newsgroup: An online discussion group that communicates about a particular subject with notes written to a central internet site and redistributed through Usenet, a worldwide network of news discussion groups.

Official state duties: Official duty means those duties within the specific scope of employment of the state officer or state employee as defined by the officer's or employee's agency or by statute or the state Constitution. ([RCW 42.52.010](#) [12])

Social media: Refers to interactive web-based technologies used for social networking and for sharing, discussing, and/or developing content. Types of social media include, but are not limited to, blogs, video- or photo-sharing sites, and social networking sites. Examples of social media sites include YouTube, Flickr, Twitter and Facebook.

Social networking: Refers to the use of social media for connecting with others and/or building online communities.

Streaming video or audio: Streaming is the process of moving images or sounds in a continuous stream over the internet in compressed format to be displayed or played when they arrive. With streaming, a web user does not have to wait to download a large file before seeing the video or hearing the sound. The user needs a player, which is a special program that decompresses and sends video data to the display and audio data to the speakers.

ESD technology resources means department owned, controlled, or provided telecommunications services (both wired and wireless) and equipment, voice (including the state SCAN network) and data networks, internet access, electronic conferencing, messaging, and e-mail systems.

POLICY:

A. Responsibility

Management must ensure that employees, business partners, contractors, and vendors using or accessing the department's computing and communications resources receive an orientation on the appropriate use of state resources and that requirements for compliance with this policy is reflected in appropriate contracts/agreements.

Employees represent the department when using computing and communications resources to conduct state business. Employees must use these tools in accordance with [Washington State Executive Ethics](#) law and applicable ethics rules.

B. Employee Use of Electronic Messaging Systems and the Internet

1. **Permitted Business Use** - Department provided electronic messaging systems and internet access may be used only to conduct business that is reasonably related to official state duties. Use of social media is subject to the department's Social Media Policy.
2. **Permitted Personal Use** - Human resources and benefits applications and websites provided by the department and other state agencies may be used. Personal use of ESD computing and communications resources must conform to WAC [292-110-010](#), Use of State Resources, which states that employees may make occasional, limited personal use of state resources such as electronic messaging systems and the internet if the use conforms to all of the following ethical standards:
 - a. There is little or no cost to the state;
 - b. The use does not interfere with the performance of the employee's official duties;

- c. The use is brief in duration and frequency. Employees are expected to exercise good judgment in both duration and frequency;
 - 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 information or software.
3. **Prohibited Uses** - Employees may never use state provided computing and communication resources in any of the following ways:
- a. Personal use of state provided electronic messaging systems or internet access that does not meet the conditions described above in Section [B.2.a-e](#) is prohibited.
 - b. Employees may not derive personal benefit or financial gain from the use of state provided e-mail, voice mail, or internet access.
 - c. Employees may not use state provided e-mail, voice mail, or internet access to conduct activities that support or are associated in any way with outside employment.
 - d. Employees must not use state provided electronic messaging systems or internet access to create, access, post, send, or print any sexually explicit, obscene, or pornographic material unless the material is necessary for the performance of the employee's job related duties (e.g., when necessary for conducting an investigation). If any such use is necessary for the performance of job related duties, employees must get written permission from their assistant commissioner or director authorizing such use.
 - e. Department employees must not use state provided internet access to connect to internet sites or create, transmit or store electronic messages that contain or promote:
 - (1) Discrimination on the basis of age, race, color, gender, creed, marital status, national origin, disability, religion, sexual orientation or Disabled and Vietnam Era Veterans status;
 - (2) Harassment or threats;
 - (3) Copyright infringement or violations of software licensing agreements;
 - (4) Personal religious beliefs;
 - (5) Political campaigns, initiatives or personal political beliefs;
 - (6) Personal business interests, including commercial uses such as

- advertising or selling; or
 - (7) Any activity that is prohibited by federal, state or local law, or department policy.
- f. In addition, employees may not use state-provided internet access to:
 - (1) Order or sell items on the internet, except as specifically approved by ESD for business purposes or sponsored activity;
 - (2) Participate in any non Employment Security sponsored online game, contest, promotion, or sweepstakes for personal financial gain;
 - (3) Participate in non work related instant messaging, email lists, blogs or newsgroups;
 - (4) Gambling or related gaming activities;
 - (5) Solicit money for religious or political causes, or for non ESD events;
 - (6) Create, post, transmit, connect to or voluntarily receive offensive, libelous, threatening or harassing material (except as related to official ESD authorized activities);
 - (7) Link ESD web (internet or intranet) sites to non-governmental internet sites that are not reasonably related to ESD programs or services, nor any website that may exhibit hate, bias, discrimination, specific religious views or advocate social or political agendas;
 - (8) Spread malware, gain unauthorized access to another computer, make another network unusable by intentionally disrupting connections to prevent access to a service or “flooding” a network to prevent legitimate network traffic;
 - (9) Transmit unencrypted sensitive or confidential department information over the internet;
 - (10) Conduct personal banking or financial transactions unless directly associated with state agency applications or websites such as Washington State Department of Retirement Systems; or
 - (11) Access social media accounts for personal use.
- g. Employees must not use state provided electronic messaging systems to make requests for disclosure of public records for personal use or benefit. Public records requests, more often than not, require additional time and resources beyond a single email and therefore are not de minimus.
- h. Employees must not establish an internet connection to or from a computer connected to the department network that bypasses the department's firewall security infrastructure or otherwise attempt to bypass or circumvent security measures put in place by ESD.

- i. Accessing personal web based email accounts or personal instant messaging services using department computers, networks and communication lines is prohibited. Transmitting department data or conducting department business via personal email or cloud storage is prohibited. Employees may not use or install email or messaging software on department computers other than those provided and supported by the department. Exceptions to this section (3)(i) may be granted where necessary for the performance of the employee's job related duties (e.g., when necessary for conducting an investigation). If any such use is necessary for the performance of job related duties, employees must get written permission from their assistant commissioner authorizing such use.
- j. Employees must not create, forward or store electronic messages in locations, including but not limited to, local computer storage, Vault, and/or Exchange Inbox that do not pertain to the state's business except as allowed in [B.2](#). This includes, but is not limited to, hoaxes, hypes, chain letters, and spamming messages to/from any computing and communications resources.
- k. Employees must not use department computing and communication resources to transmit/receive streaming video or audio unless it is required for work related purposes. If viewing or listening is required, it should be of limited use and coordinated as a group running a single copy to minimize the impact to department network resources.
- l. Employees must not use department computing and communication resources to make personal long distance phones calls, regardless of duration.
- m. Employees must not connect non ESD managed computing and communications resources to ESD networks, except via ESD provided remote access services (e.g. VPN) or with the prior written authorization of the Information Technology security manager.

C. Usage Based Services

Charges for services that are billed on an individual user basis, such as wireless services or SCAN telephone services, will be available for electronic review by the individual user of record and their immediate supervisor. If a discrepancy is identified, the user must identify any charges not incurred in support of legitimate state business. The electronic detail will be retained following ESD's record retention schedule.

D. Passwords

Passwords, PIN codes, and other similar methods of securing ESD computing and communication resources are assigned to individual users. They should be kept confidential and never be shared.

E. Distribution Lists

Department wide distribution lists are intended for executive leadership level use. The ESD Service Desk at 1-877-397-1212 can assist department staff in developing distribution lists that will reach the appropriate target audience without generating unnecessary message traffic.

F. Monitoring, Enforcement, and Disciplinary Action for Noncompliance

Nothing contained in this policy shall be construed to create a right of privacy in any content transmitted via the department's electronic messaging systems. The department may monitor and log all activity on ESD computing and communication resources, including, but not limited, to internet access. ESD monitoring and logging may be used by the department for any purpose.

The Information Technology and Business Integration Division (ITBI) has the responsibility of managing content filtering in accordance with this policy and agency operational considerations. All employees will be placed in a default content filtering group by ITBI. A current list of site categories and their treatment by the ESD internet filter is available by contacting [ITBI Enterprise Systems and Storage](#). Exceptions (either more permissive or restrictive) to standard content filtering are granted by the request of their assistant commissioner or director. Staff are to direct requests through their supervisor to their assistant commissioner or director, who submits them to the Information Technology and Business Integration Division's service desk. Computers intended for public use (e.g. WorkSource Resource rooms) may be filtered differently than employee use accounts and machines. Not all sites available through the internet filter may be allowable under this policy.

Violations of this policy may result in disciplinary action, up to and including dismissal from employment. In addition, there may also be separate actions against an employee for violation of the state's ethics laws such as letters of reprimand, fines, restitution, civil actions, and criminal prosecution.

Employment Security has zero tolerance for pornographic and sexually explicit materials as described above in B.3.d. If, after a just cause investigation, it is found that an employee used state-provided electronic messaging and/or the internet to create, access, post, send, or print any sexually explicit or pornographic material in violation of this policy, it will result in termination of an individual's employment with the department. In addition, the individual may be subject to other legal consequences for violating

additional state or federal laws.

G. Illustrative Examples of Permitted and Prohibited Use

Example 1: An employee makes a local telephone call or sends an email communication to her home to make sure her children have arrived safely home from school. This is not a violation of this policy. There is no cost to the state and because the call or email is brief in duration, it does not interfere with the performance of official duties.

Example 2: An employee uses his agency computer to send electronic mail to another employee regarding the agenda for an agency meeting that both will attend. He also wishes the other employee a happy birthday. This is not a violation of this policy. The personal message is brief and improves organizational effectiveness by allowing informal communication among employees.

Example 3: Several times a month an employee quickly uses the internet to check his children's school web site to confirm if the school will end early that day. The inquiry takes about five minutes. This is not a violation of this policy. The use is brief and infrequent, there is little or no cost to the state and the use does not interfere with the performance of official duties.

Example 4: An employee routinely uses the internet to manage her personal investment portfolio and communicate information to her broker. This is a violation of this policy. Using state resources to routinely monitor private stock investments, make stock trades or to make any bank or other financial transaction that can result in a private financial benefit or gain. Allowing even an occasional or limited use of state facilities to facilitate a private financial gain undermines public confidence in state government.

Example 5: An employee spends thirty minutes or more looking at various web sites related to personal interest. This is a violation of this policy. The use is not brief and can interfere with the performance of state duties.

Example 6: An employee visits several humor and joke sites. While at a site, he downloads a joke file and emails it to several co-workers. This is a violation of this policy. By emailing a file to coworkers, the employee disrupts other state employees and obligates them to make a personal use of state resources. In addition, downloading files and distributing them to coworkers can introduce a computer virus, which can compromise state databases.

Example 7: An employee uses state provided internet to access state provided benefits on Department of Retirement Systems, Deferred Compensation Plan, Health Care Authority or Department of Personnel Web sites for reasons such as:

- Updating personal information;
- Reviewing information about state retirement benefits;

- Reviewing or updating account allocations in a state provided retirement benefit plan;
- Selecting among health care benefit options;
- Reviewing job postings or submitting job applications;
- Registering for training opportunities; or
- Requesting assistance from a variety of programs and services available to state employees (such as disability accommodation assistance, recruitment and diversity program specialists, and the Employee Advisory Service).

Such actions are not violations of the policy as long as they conform to the ethical standards found in [Section B.2](#) of this policy. All of the activities above are part of the diverse benefits package available to state employees and are directly related to state employment. Reviewing and updating information on these web sites facilitates the efficient administration of employee benefits statewide. Prohibiting state employees from using agency provided internet access for this purpose would undermine the efficiencies and savings achieved by widespread access to the web sites.

SUPERSEDES:

ADMINISTRATIVE POLICY AND PROCEDURE 2009
USE OF TELECOMMUNICATIONS TECHNOLOGY SYSTEMS
DATED 05/01/02

ADMINISTRATIVE POLICY AND PROCEDURE 2016
ACCEPTABLE USE OF COMPUTING AND COMMUNICATIONS RESOURCES
DATED 06/04/13

RELATED POLICIES:

Social Media Policy #0035

DIRECT INQUIRIES TO:

INFORMATION TECHNOLOGY AND BUSINESS INTEGRATION DIVISION
Infrastructure Services Deputy Director
(360) 407-4764