**Administrative Policy No. 15.15**

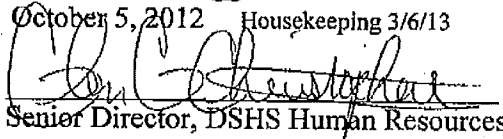
Subject: Use of Electronic Messaging Systems and the Internet

Information Contact: DSHS Human Resources

Authorizing Source: RCW 42.52 (Ethics in Public Services)
RCW 49.60.010 (Law Against Discrimination)
WAC 292-110-010 (Use of State Resources)
DSHS Administrative Policies
18.66 (Discrimination and Harassment Prevention)
18.68 (Employee Participation in Political Activities)
18.64 (Standards of Ethical Conduct for Employees)

Effective Date: July 1, 1991

Revised: October 5, 2012 ⁱⁱ Housekeeping 3/6/13

Approved By: 
Senior Director, DSHS Human Resources

Sunset Review Date: October 5, 2014

Purpose

Establishes the Department of Social and Health Services (DSHS) policy regarding the use of electronic messaging systems and the Internet. Electronic messaging systems and the Internet 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 department employees, contractors, interns, vendors, volunteers, and business partners who have access to department networks or use the department's electronic messaging systems and/or have Internet access.

Additional Guidance

Voice mail messages, email messages, and Internet use histories are public records and subject to public records disclosure or legal discovery unless privileged or specifically exempt by law. Electronic documents, including email messages are subject to record retention requirements. Policies related to information technology security, public records disclosure, discovery, and records retention that apply to electronic messaging systems and Internet usage can be found in the DSHS Information Technology Security Policy Manual, Administrative Policy 5.02, and Administrative Policy 5.04.

APPROVED

<http://asd.dshs.wa.gov/RPAU/documents/Admin-Policy/15-15.htm> **Executive Ethics Board** 4/2/2013

Date: 9.13.13

Additional information and guidance related to the appropriate use of state resources is on the Executive Ethics Board website

Definitions

Confidential Information: Information protected by state or federal laws including information about DSHS clients, employees, interns, volunteers, vendors or contractors, and department systems.

Department: The Department of Social and Health Services.

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

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

Employee: A DSHS employee with access to department electronic messaging systems or department supplied Internet access.

Encryption: The translation of data into a secret code. A secret key or password is required to enable decryption. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

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 create a private chat room with another individual. Typically, the instant messaging system alerts the person whenever somebody on his or her private list is online. He or she can then initiate a chat session with that particular individual.

Internet: An unsecured publicly accessible network.

ListServ: A system that automatically redistributes email to names on a mailing list. Users subscribe by sending an email note to a listserv. The system automatically adds the user's name and distributes future user email postings to them and every other subscriber.

Malware (abbreviation for malicious software): Software specifically designed to damage or disrupt a system, such as a virus, worm, or Trojan horse.

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: Those duties within the specific scope of employment of the state officer or state employee as defined by the officer or employee's agency or by statute or the state Constitution. (RCW)

APPROVED

<http://asd.dshs.wa.gov/RPAU/documents/Admin-Policy/15-15.htm>

Executive Ethics Board 4/2/2013

Date: 9.13.13

42.52.010(12))

Pornographic Materials: The explicit representation of the human body or sexual activity with the goal of sexual arousal and/or sexual relief. These materials connote the more direct, blunt, or excessive depiction of sexual acts, with little or no artistic value, intended for mere entertainment.

Sexually Explicit Materials: Video, photography, creative writing, films, magazines, or other materials intended primarily to arouse sexual desire or cause sexual arousal.

Social Media: Social media, used for social networking, refers to providers or services that use the Internet for blogging, photo and video sharing, wikis, discussion boards and social and professional networking. This does not include social media located within the DSHS intranet (e.g. Blog Central, IESA).

Streaming Video or Audio: 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. 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 special program that decompresses and sends video data to the display and audio data to the speakers.

Policy

A. Responsibility

Supervisors and managers are required to ensure that employees, business partners, contractors, interns, volunteers, and vendors with access to the department's electronic messaging systems and/or the Internet have been instructed and trained on the appropriate use of state resources.

Upon DSHS employment, all employees with Internet access must read and sign DSHS 03-344, Internet Access Request and Agreement, acknowledging that they understand the department's policy. The signed form must be kept in the employee's local personnel file. The form is available at http://asd.dshs.wa.gov/forms/wordforms/word/03_344.doc.

B. Lack of Privacy

Whenever state-provided electronic messaging systems are used, there should be no expectation of privacy. Records created by these systems may be requested by anyone under the Public Records Act and may need to be produced in "discovery" or during the litigation process. Public records staff who review these records only redact or withhold information specifically exempt by law and do not use a personal privacy standard to determine what is not provided to requestors. When appropriate, employees whose records are the subject of a public records request may be notified under Administrative Policy 5.02 and have the opportunity to seek court action to enjoin disclosure of parts of these records.

As authorized by DSHS policy or by the Secretary/Designee, any portion of a user's electronic messaging system, including email or Internet history, may be accessed without consent of the sender or recipient as needed to carry out DSHS business functions, in the course of an audit, or if there is reason to believe misuse has occurred. An agency manager has the authority to monitor employee use of internet. If an employee has used personally-owned systems or devices to do DSHS work, those records are also subject to access. Records obtained without the consent of the sender or recipient may be used as the basis for disciplinary action.

APPROVED

<http://asd.dshs.wa.gov/RPAU/documents/Admin-Policy/15-15.htm>

Executive Ethics Board 4/2/2013

Date: 9.13.13

C. Employee Use of Electronic Messaging Systems and the Internet

1. **Permitted Business Use** - Employees may use department provided electronic messaging systems and Internet access to conduct business that is related to official state duties, to include electronic recruiting and Employee Self Service.

Employees represent DSHS when using electronic messaging systems and accessing the Internet to conduct state business. Employees must use these tools in accordance with Administrative Policy 18.64, Standards of Ethical Conduct for Employees.

2. **Permitted Personal Use**

Personal use of department electronic messaging systems and the Internet must conform to WAC 292-110-010, Use of State Resources, which states that employees may make occasional and 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 personal use of state resources; and
- e. The use does not compromise the security or integrity of state information, computer equipment or software.

3. **Prohibited Uses** – Employees are prohibited from using state-provided electronic messaging systems and the Internet in any of the following ways:

- a. Personal use of state-provided electronic messaging systems or Internet access that does not meet the conditions found in C.2.a-e above is prohibited.
- b. Employees may not use state resources for personal benefit or gain. Or for the benefit or gain of other individuals or outside organizations.
- c. Employees must not use state-provided email, voice mail, copying, imaging, or Internet access to conduct activities that support outside employment.
- d. Employees must not use state-provided electronic messaging systems, faxing, scanning, or Internet access to create, access, post, send, or print any 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 such use is necessary for the performance of job-related duties, employees must receive written permission from their supervisor authorizing such use.
- e. Department employees must not use state-provided Internet sites, faxing, scanning, or copying to 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, use of a trained guide dog, or service animal by a person with a disability, religion, sexual orientation, disabled veteran, Vietnam Era Veteran status, recently separated veteran, or other protected veteran status;

APPROVED

Executive Ethics Board 4/2/2013

Date: 9.13.13

- 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;
 - 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 DSHS for business purposes;
 - 2) Participate in any online game, contest, promotion, or sweepstakes;
 - 3) Participate or post in non-work related Instant Messaging, Social Media, ListServ, or newsgroups;
 - 4) Gamble;
 - 5) Solicit money for religious or political causes, or for non-DSHS events;
 - 6) Create, post, transmit, connect to, or voluntarily receive offensive, libelous, threatening, or harassing material (except as related to official DSHS authorized activities);
 - 7) Link DSHS web sites to other Internet sites in violation of Administrative Policy 15.18;
 - 8) Spread malware, make another network unusable by intentionally disrupting connections to prevent access to a service or "flooding" a network to prevent legitimate network traffic;
 - 9) Gain unauthorized access to another computer;
 - 10) Transmit unencrypted sensitive or confidential department information over the Internet; or
 - 11) Upload or email files or programs that can cause harm to the network.
- g. Employees must not use state provided electronic messaging systems to make requests for disclosure of public records for personal use or benefit.
- h. Employees must not establish an Internet connection (e.g., AOL, MSN, etc.) to or from a computer connected to the department network that bypasses the Washington State Department of Information System (DIS) firewall.
- i. Checking personal and/or outside non-DSHS email accounts using department computers, and/or the State Government Network is prohibited. Employees must not use email products on department computers other than those provided and supported by the department.
- j. Using instant messaging provided by external vendors is prohibited. This includes instant messaging solutions offered by vendors such as Microsoft, AOL, and Yahoo.
- k. Employees must not create, forward, or store electronic messages that do not pertain to the state's business except as allowed in C.2. This includes, but is not limited to, hoaxes, hypes, chain letters, and spamming messages.
- l. Employees should not attempt to access networks through hacking or visiting hacker websites.
- m. Employees who are on the DSHS Wide Area Network must not use streaming video/audio, Internet radio, net meeting or other audio/video training or live legislative broadcasts unless it is required for work related purposes. If viewing

APPROVED

or listening is required, it should be of limited use and coordinated as a group running a single copy to minimize the impact to the DSHS Wide Area Network.

If an employee inadvertently accesses an inappropriate site while using the Internet, the employee should immediately close the page and notify his or her supervisor.

D. Distribution Lists

Employees may not use an email distribution list that attempts to cover all state employees or state agencies and may not use an "All DSHS" list. The Secretary/Designee will establish who can send to the DSHS "all staff" email distribution list. The ISSD Help Desk at (360) 902-7700 or 1-888-329-4773 can assist DSHS staff in developing distribution lists that will reach the appropriate target audience without generating unnecessary message traffic.

E. Disciplinary Action for Noncompliance

1. Violations of this policy may result in disciplinary action, up to and including termination from state 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, civil actions, and criminal prosecution.
2. Pornographic Materials: DSHS has a zero tolerance regarding pornographic material in the workplace. If an investigation determines an employee used state resources to create, access, post, transmit, print, or store pornographic materials not appropriate for the workplace, the most stringent disciplinary action will be taken.
3. Sexually Explicit Materials: If an investigation determines an employee used state resources to create, access, post, transmit, print, or store sexually explicit materials not appropriate for the workplace, appropriate disciplinary action will be taken, up to and including termination from DSHS employment. The administration's highest-level appointing authority will consult with the Senior Director of DSHS Human Resources to determine the level of disciplinary action taken.
4. If a contractor used state resources to create, access, post, transmit, print, or store pornographic or sexually explicit materials, DSHS will take appropriate action as provided in the contract.

F. Examples of Permitted and Prohibited Use

Example 1: An employee sends an email to his or her home to make sure his or her children have arrived home safely from school. **THIS IS NOT A POLICY VIOLATION.**

- There is no cost to the state;
- The phone call or email is brief in duration; and,
- It does not interfere with the performance of official duties.

Example 2: An employee uses his or her state computer to send electronic mail to another employee regarding the agenda for an agency meeting that both will attend. In the same email he or she also wishes the other employee a happy birthday. **THIS IS NOT A POLICY VIOLATION.**

- The personal message is brief;
- There is no cost to the state; and
- It does not interfere with the performance of official duties.

Example 3: An employee checks the Internet site for their child's school two or three times per month for updates on early dismissal. Each transaction takes two to three minutes. **THIS IS NOT**

APPROVED

<http://asd.dshs.wa.gov/RPAU/documents/Admin-Policy/15-15.htm> Executive Ethics Board 4/2/2013

Date: 9.13.13

A POLICY VIOLATION.

- 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 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;
- Review 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 Assistance Program.

THIS IS NOT A POLICY VIOLATION, as long as they conform to the ethical standards found in Section C.

- All of the activities above are part of the diverse benefits package available to state employees and are directly related to state employees and their 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.

Example 5: An employee routinely uses the Internet to manage his or her personal investment portfolio and communicate information to his or her broker. **THIS IS A POLICY VIOLATION.**

Using state resources to monitor private stock investments or make stock trades are private activities that can result in a private financial benefit or gain. Allowing even an occasional or limited use of state resources to facilitate a private financial gain undermines public confidence in state government.

Example 6: An employee spends thirty to forty minutes looking at various web sites related to personal interest. **THIS IS A POLICY VIOLATION.**

Although the web sites may be permissible, the use is not brief and can interfere with the performance of official duties.

Example 7: An employee visits several humor and joke sites. While at a site, he or she downloads a joke file and emails it to several co-workers. **THIS IS A POLICY VIOLATION.**

- Visiting such sites is prohibited;
- Emailing a file to a co-worker distracts him or her from official duties and obligates that employee to report the misuse to his or her supervisor; and
- Downloading files and distributing them to co-workers can introduce a computer virus,

APPROVED

<http://asd.dshs.wa.gov/RPAU/documents/Admin-Policy/15-15.htm> Executive Ethics Board 4/2/2013

Date: 9.13.13

which can compromise state databases.

(i) Removed references to requiring prior approval