Washington State
DEPARTMENT OF
SOCIAL & HEALTH
SERVICES

ADMINISTRATIVE POLICY NO. 15.15

SUBJECT: Use of Electronic Messaging Systems and the Internet

INFORMATION CONTACT: IT Security Administrator
Information System Services Division
MS 45889 (360) 902-7550 FAX (360) 902-7529

AUTHORIZING SOURCE:
Code of Federal Regulation (CFR)
Title 36, Electronic Mail, Parts 1220, 1222, 1228, & 1234
Public Law 99-508 (18 USC §2510 et seq. Electronic Communications Privacy Act of 1986)
Revised Code of Washington (RCW)
- 40.14 (Public Records)
- 42.17 (Public Disclosure)
- 49.60.010 (Law Against Discrimination)

Washington Administrative Code (WAC)
- 292-110-010, Use of State Resources

Washington State Records Retention General Schedule GS-17)
DSHS Administrative Policies
6.04, Standards of Ethical Conduct for Employees
6.14, Public Disclosure

EFFECTIVE DATE: May 15, 1991

REVISED September 1, 2002

APPROVED BY:

SUNSET REVIEW DATE: September 1, 2004

PURPOSE:

This establishes the department's policy regarding the use of Department of Social and Health Services (DSHS) 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. It also identifies requirements for creating and updating user information.

APPROVED
Executive Ethics Board
Date: 4/11/03

SCOPE:

This policy applies to all department employees and contractors having access to our networks and using the department's electronic messaging systems and/or having Internet access. Administrations/Divisions may choose to develop more stringent policies, provided their employees are notified in writing sufficiently in advance to be aware of changes.

ADDITIONAL GUIDANCE:

Additional procedures and guidelines may be found in the DSHS Information Technology Security Policy Manual.

DEFINITIONS:

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 or typed communication. These messaging systems are commonly referred to as voice mail and e-mail respectively.

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

Hoaxes, Hypes, Chainletters 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/her private list is online. He/she can then initiate a chat session with that particular individual.

APPROVED
Executive Ethics Board
Date: 4/11/03

POLICY:

A. **Responsibility**

Management should ensure that employees, business partners, contractors, and vendors having access to the department's electronic messaging systems and/or the Internet receive an orientation on the systems and the appropriate use of state resources.

All DSHS 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. **Employee Use of Electronic Messaging Systems and the Internet**

1. **Permitted Business Use** – Department staff may use electronic messaging systems and Internet access to conduct business that is reasonably related to official state duties.

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 6.04, Standards of Ethical Conduct For Employees.

2. **Permitted Personal Use** - WAC 292-110-010, Use of State Resources, states that department employees may make occasional but limited personal use of state resources such as electronic messaging systems and the Internet if the use conforms to the following ethical standards:

   a. There is little or no cost to the state; and

   b. The use does not interfere with the performance of the employee's official duties; and

   c. The use is brief in duration and frequency. Employees are expected to exercise good judgment in both duration and frequency; and

   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** – Department staff are prohibited from using state-provided electronic messaging systems and the Internet in the following ways:

   a. Personal use of state-provided electronic messaging systems or Internet access that does not meet the conditions found in B.2.a-e is prohibited.

   b. Employees may not derive personal benefit or gain from the use of state provided e-mail, voice mail, or Internet access.

   c. 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;

      (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

APPROVED
Executive Ethics Board
Date: 4/11/03

(7) Any activity that is prohibited by federal, state or local law, or department policy.

d. In addition, staff 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 in non-business related Instant Messaging, chat groups, list servers (automatic distribution lists), 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 obscene, pornographic, offensive, libelous, threatening or harassing material (except as related to official DSHS investigative activities);

(7) Link DSHS Web sites to other Internet sites in violation of Administrative Policy 15.17, External Content on DSHS Web Sites;

(8) Store department data on disk storage devices operated by vendors over the Internet;

(9) Spread viruses, gain unauthorized access to another computer, or make another network unusable by launching a denial of service attack; or

APPROVED
Executive Ethics Board
Date: 4/11/03

(10) Transmit unencrypted sensitive or confidential department information over the Internet.

e. Employees will not establish an Internet connection (e.g., AOL, MSN, etc.) to or from a networked station that bypasses the Washington State Department of Information Services (DIS) firewall.

f. Checking personal, outside e-mail accounts using department computers, networks and communication lines is prohibited. Employees will not use e-mail products on department computers other than those provided and supported by the department. Examples of prohibited products include e-mail accounts offered by Hotmail, Yahoo, Earthlink, MSN and AOL.

g. Employees will not create, forward or store electronic messages that do not pertain to the state's business except as allowed in B.2. This includes, but is not limited to, hoaxes, hypes, chainletters, and spamming messages.

h. Employees who are on the DSHS Wide Area Network will not use streaming video or audio, Internet radio, net meeting or other audio/video training or live

legislative broadcasts 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 the DSHS Wide Area Network.

C. **Public Disclosure and Retention**

1. Voice mail messages, e-mail messages and Internet usage histories are public records and subject to requests for public record disclosure in accordance with public records law in Chapters 42.17 RCW and 388-01 WAC.

2. E-mail retention is the responsibility of the sender and receiver of the e-mail message. Employees must follow the DSHS and state retention schedules for records of the same nature and purpose when deciding whether to retain e-mails. Employees should periodically review their electronic files for destruction or archiving in accordance with Appendix C of the State General Retention Schedule.

D. **Protecting Confidential E-Mail Messages**

1. DSHS employees must protect transmitted messages or files containing confidential or privacy-protected information (e.g., confidential client or employee data) to ensure there is no unauthorized access. The message or file:

   a. Must be encrypted if transmitted outside the department's trusted State Government Network (SGN) using the DSHS secure e-mail message system. In most cases, if the e-mail address is listed in the global address listing, additional encryption is not required; and

   b. May not be forwarded or shared, except as allowed by law.

2. Senders and receivers of all DSHS confidential information are responsible for ensuring the information is not disclosed.

E. **Distribution Lists**

Employees may not use an e-mail distribution list that attempts to cover all state employees or agencies and must avoid using an "all DSHS" distribution list. The ISSD Help Desk at (360) 586-HELP 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.

F. **User Information**

Each division director or the division designee(s) must ensure that the following policies are enforced within their area of responsibility:

1. The following user information must be maintained in the e-mail properties for each employee in accordance with the Statewide Exchange Administrators Naming Conventions Guidelines:

   - Last name, first name
   - Display name

- Job Title
- Company = DSHS (Available on the Exchange system only)
- Office telephone number including area code
- Fax number including area code
- Mail Stop or indicator if none
- Complete mailing address
- Department = Division/Administration
- Office

2. Additions or changes to employee e-mail properties must be completed within two weeks from the effective date of the addition or change.

G. **System Monitoring**

1. Existing messages residing on department electronic messaging systems are state property and subject to access by an employee's appointing authority or designee upon written request to the appropriate system administrator.

2. LAN managers or ISSD may monitor electronic messaging system usage at the discretion or request of department management.

H. **Recurring Internet Policy Messages**

Directors must ensure that employees with Internet access are regularly advised of the permitted and prohibited uses of state provided Internet access. For example, during the computer boot-up process or when the Internet browser launches, network administrators should display the following message: "Internet access is provided to employees to conduct state of Washington business. Personal use of the Internet is limited and strictly governed by department policy and state ethics law."

I. **Disciplinary Action for Non-compliance**

Violations of this policy may result in disciplinary action, up to and including dismissal from employment or more serious consequences (e.g., criminal charges).

APPROVED
Executive Ethics Board
Date: 4/11/03

J. **Examples of Permitted and Prohibited Use**

EXAMPLE 1. An employee makes a local telephone call or sends an e-mail 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 e-mail 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 transaction 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 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 facilities to facilitate a private financial gain undermines public confidence in state government.

EXAMPLE 5. An employee spends thirty to forty minutes 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 e-mails it to several co-workers. This is a violation of this policy. By e-mailing a file to co-workers, 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 co-workers can introduce a computer virus, which can compromise state databases.

APPROVED
Executive Ethics Board
Date: 4/11/03