

STATE OF WASHINGTON  
EMPLOYMENT SECURITY DEPARTMENT  
POLICY AND PROCEDURE

NUMBER: 2016  
PAGE: 1 OF 8  
DATE: 04/16/03

**SUBJECT:** Use of Department Information Technology Resources<sup>1</sup>

**PURPOSE:**

To set forth the Employment Security Department's (department) position regarding the proper business and personal use of department information technology resources, including electronic mail, and the Internet by employees.

**STEWARDSHIP:**

Employment Security Department employees are obligated to conserve and protect state resources for the benefit of the public interest rather than their private interests. The rationale for this policy is the need to maintain public trust and confidence in state services and protect the integrity of state information technology resources and systems. This policy will help limit risk and liability to both the department and the individual employee. Potential risks and liabilities associated with the use of the department's information technology resources include:

- Loss of public trust and confidence in department/state services;
- Service and performance interference;
- Financial loss;
- Illegal activity;
- Loss of network or operational integrity; and
- Charges or other legal consequences related to sexual harassment, racism, or improper access to or dissemination of information.

**DEFINITIONS:**

**Information technology resources** include, but are not limited to, information technology assets such as computers, workstations, data resources, hand held computing devices, electronic message systems, networks, business applications/systems, software, software licenses, and Internet connections or accounts.

**Electronic message** is a verbal or written message transmitted or stored electronically.

**APPROVED**  
**Executive Ethics Board**

Date: 5/9/03

<sup>1</sup> The Executive Ethics Board has reviewed and approved this policy per RCW 42.52.360 (4) in formal session on *(include date)*. The Executive Ethics Board adopted rules in WAC 292-110-010, as well as, the state's Ethics in Public Service law (RCW Chapter 42.52) which provided direction for the guidance given in this information technology policy.

**Electronic message systems** allow the generation, transmission, storage, display or reproduction of an electronic message for internal or external communication purposes.

- Voice mail is a system allowing users to receive, reply, redirect, save or send messages anytime using a touchtone telephone.
- E-mail is a system allowing transmission of person-to-person messages.
- Other media includes facsimile and imaging equipment, which store and transmit images, and all similar systems.

**Internet** means the connection to and use of interconnected networks in the public and private domains to access the World Wide Web, Gopher, file transfer protocols and other network resources.

**Intranet** is a private network for internal communication that may have links to the Internet. The department's intranet site is <http://insideesd.esd.wa.gov/>.

**Non-working hours** means those hours before and after scheduled work hours for the scheduled employee, those hours other than designated working hours for non-scheduled employees, and breaks, including lunch breaks, for both the scheduled and non-scheduled employees.

**POLICY:**

The Employment Security Department is a strong proponent of the responsible, legal and ethical use of information technology. Our ability to use these tools greatly enhances our mission and makes us more efficient when dealing with information gathering and exchange. We encourage all of you to use these technologies, keeping in mind the principles explained below.

Regardless of the specific technology employed, the use of information technology must comply with this policy. Department management is responsible for ensuring that employees and other individuals with access to the department's electronic systems and/or the Internet are informed of this policy and make appropriate use of state resources in accordance with this policy.

The department has the right to access information technology equipment and any information stored on it for any legitimate business purpose including, but not limited to, the promotion and assessment of compliance with this policy.

Violation of this policy may subject the employee to disciplinary action by the department and to sanctions that may be imposed by the Washington State Executive Ethics Board, including financial penalties.

**APPROVED**  
**Executive Ethics Board**  
Date: 5/9/03

INFORMATION TECHNOLOGY AS A STATE RESOURCE

The department's information technology resources are state resources. They may not be used for personal benefit or gain or for the benefit or gain of other individuals or outside organizations. Personal benefit or gain may include a use solely for personal convenience, or a use to avoid personal expense. Refer to WAC 292-110-010 Use of State Resources and Examples and Frequently Asked Questions for more information.

When all of the following conditions are met, department employees may make occasional but limited personal use of the department's information technology resources (excerpts from WAC 292-110-010(3):

- There is little or no cost to the state;
- Any use is brief in duration, occurs infrequently, and is the most effective use of time or resources;
- The use does not interfere with the performance of the employee's official duties;
- The use does not disrupt or distract from the conduct of state business due to volume or frequency;
- The use does not disrupt other individuals and does not obligate them to make a personal use of state resources; and
- The use does not compromise the security or integrity of state property, information, or software.

Occasional and limited use of the department's information technology resources may not include the following private uses (excerpts from WAC 292-110-010(6)):

- Any use for the purpose of conducting an outside business, or private employment;
- Any use for the purpose of supporting, promoting the interests of, or soliciting for an outside organization or group, including but not limited to: a private business, a non-profit organization, or a political activity (unless provided for by law or authorized by an agency head or designee);
- Any use for the purpose of assisting a campaign for election or for the promotion of or opposition to a ballot proposition;
- Any use for the purpose of participating in or assisting in an effort to lobby the state legislature, or a state agency head (unless provided for by law or authorized by an agency head or designee);
- Any use related to conduct that is prohibited by a federal or state law or rule, or a state agency policy; and

**APPROVED**  
**Executive Ethics Board**

Date: 5/9/03

**USE OF DEPARTMENT INFORMATION  
TECHNOLOGY RESOURCES**

**NUMBER: 2016  
PAGE: 4 OF 8  
DATE: 04/16/03**

- Any private use of any state property [like a laptop computer], that has been removed from state facilities or other official duty stations, even if there is no cost to the state.

As state resources, the department's information technology resources may never be used to:

- Adversely reflect on the department e.g., furthering of extremist organizations, inappropriate jokes, chain letters, or gender slurs;
- Engage in any commercial activity including advertising, selling or purchasing goods and services;
- Monitor private stock investments or make stock trades or similar private activities that can result in a private financial benefit or gain;
- Make unlawful or inappropriate disclosures of confidential information;
- Play computer games, other than those preloaded by the manufacturer and approved for use for training, during working or non-working hours;
- Promote a political, philosophical or religious belief;
- Promote or encourage discrimination on the basis of race, creed, color, gender, religion, handicap, or sexual orientation; or
- Express inappropriate or abusive language;

**INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE:**

Information technology equipment and software is provided by the department to assist its employees in the performance of their duties. This equipment and software shall be used only for purposes consistent with those enumerated in this policy.

Security of department information technology resources and the data they contain is the responsibility of all users. Access to department information technology resources and systems are authorized only to the level necessary for performance of an employee's job functions. Attempting to circumvent data protection schemes, unauthorized monitoring, or tampering with another user's electronic communications is not allowed.

**APPROVED**  
**Executive Ethics Board**  
Date: 5/9/03

**USE OF DEPARTMENT INFORMATION  
TECHNOLOGY RESOURCES**

**NUMBER: 2016  
PAGE: 5 OF 8  
DATE: 04/16/03**

Software, programs, information, files and data stored on state-owned equipment are state resources and any personal information stored on this equipment is subject to review and is not private. Information stored on this equipment must be consistent with this policy. The department has the right to access information technology equipment, software and any information stored on it. This includes the promotion and assessment of compliance with this policy.

In using state owned equipment, employees shall protect the confidentiality of information by following password procedures and taking all the necessary steps to safeguard passwords. The employee's User ID and password are his or her identity when accessing and using department information technology resources. They are for that employee's use only and are not to be shared with anyone else including network and desktop support technicians or technical support organizations. An employee is responsible for actions taken with his or her User ID and password. If the employee is storing particularly sensitive information, the employee should discuss additional security with the appropriate supervisor or manager.

New or additional equipment and software may not be installed on the department's state owned information technology resources, e.g. PC's, local area networks (LANs) and wide area networks (WANs) without prior written approval from the department's Information Technology Services Division (ITSD). This includes, but is not limited to:

- Equipment that may be attached to LAN's such as, routers, hubs, switches, PC's, scanners, printers and hardware or software that gives an employee remote access to the department's LANs or the Washington State Government Network (SGN);
- CSU/DSUs, routers, circuits and switches that provide access to the SGN; and
- Wireless networks.

No equipment or software installed on the department's state owned information technology resources may be modified without prior written approval from the ITSD.

Additionally, employees must comply with copyright laws. Therefore, no unauthorized duplication of software, images, or other intellectual materials that are subject to copyright is permissible. Compliance with all state and federal laws and restrictions applying to the use of any and all copyrighted materials are to be followed.

**APPROVED  
Executive Ethics Board**

Date: 5/9/03

**INTRANET USE:**

Employees are encouraged to access the department's intranet site <http://insideesd.esd.wa.gov/>. This site contains information that is valuable for all Employment Security Department employees in the performance of their official duties. Managers have the authority to establish guidelines for appropriate use of the intranet by staff.

**INTERNET AND ELECTRONIC-MAIL (E-MAIL) USE:**

Department employees may use state computers and other equipment to access computer networks or other databases, including the Internet and electronic mail, provided such use conforms to this policy, the ethical standards under WAC 292-110-010(3) and the use is not otherwise prohibited under WAC 292-110-010(6).

Information technology resources, including Internet and e-mail, are provided by the state for the purposes of conducting department business and to assist its employees in the performance of their jobs. Occasional and limited (i.e. *de minimis*) personal use of information technology resources by department employees is permitted in accordance with this policy. Employees may have a need at times to contact family, friends, and take care of a limited amount of personal business during the workday. Carefully considered personal use of the Internet and e-mail may be a component of such permissible use, just as the telephone serves a similar purpose.

The occasional and limited use to review and update state provided benefits is permitted.

**Business Considerations:**

- Unless specifically authorized to do so, employees should not claim to represent the views or positions of the department.
- If an employee accidentally accesses a site that contains inappropriate or illegal material, she or he must leave the site immediately. If concerned, the employee may choose to notify his or her supervisor or manager.
- Inappropriate communications received via e-mail may be discussed with your supervisor or other knowledgeable individuals for action. If you receive questionable or inappropriate e-mail, notify the sender and ask to be removed from their address book or mailing list and if the sender is outside state government notify them that they have accessed a state e-mail system.
- Employees with access to department information technology resources may not use these resources to establish personal electronic mail or Internet account(s).
- When the Internet is used, the employee and the Employment Security Department are identified as the sender or recipient.
- Communications using electronic message systems should be as courteous and professional as any other written or oral communication in the workplace.

**APPROVED**  
**Executive Ethics Board**  
Date: 5/9/03

**Security Considerations:**

- The Internet is not a secure means of transmission. Communications on the Internet are not private. Unless computer applications that have been designed specifically for secure transactions are employed, sensitive or confidential files or e-mail should not be sent over the Internet as they may be captured and read by unauthorized individual(s).
- Downloading files, software or any other materials may subject the computer and the network to viruses that can destroy data on the computer and even the network.
- Employees may not bypass or attempt to bypass the Washington State Department of Information Services (DIS) firewall.

**Privacy Considerations:**

- Electronic messages generally constitute public records that are subject to disclosure under chapter 42.17 RCW.
- Internet/intranet access leaves a documented trail. Any use of state provided equipment, software, and network resources are public records and may be disclosed. Any use of the Internet/intranet is subject to review by management and both internal and external auditors and investigators.

**General Guidelines:**

These guidelines from various resources, including the state Executive Ethics Board, are provided here to assist department employees in making the correct determination of proper use of the department's technology resources:

- Electronic mail and the Internet/intranet use many of the same network resources. They can be used to communicate in a manner that is permissible under this policy.
- This policy requires the use of judgement. If there is any doubt about whether; (a) the use is occasional and limited, (b) there is little or no cost to the state, or (c) the use interferes with official business, employees should consult their supervisor. Supervisors may provide guidance for appropriate use and may restrict an employee's access to the Internet/intranet, e-mail or other information technology resources.
- If in doubt, limit your use of technology resources to **state business purposes only!**
- Never use technology in a way that would be embarrassing to the department/state.
- Use technology only in a manner you could discuss openly with your supervisor or other employees.

**APPROVED**  
**Executive Ethics Board**

Date: 5/9/03

**ADDITIONAL REFERENCES:**

WAC 292-110-010 Use of State Resources

RCW Chapter 42.52 Ethics in Public Service law

Examples and Frequently Asked Questions to help understand and apply WAC 292-110-010

Employment Security Policy and Procedure #0019 dated 05/06/01 "Fund Raising for Charitable Purposes"

Employment Security Policy and Procedure #1016 dated 07/26/02 "Employee Conduct."

Employment Security Policy and Procedure #4002 dated 01/08/96 "Microcomputer/Workstation Policy."

**SUPERSEDES:**

Employment Security Policy and Procedure #2016 dated 12/20/00 "Use of Agency Information Technology Systems."

**DIRECT INQUIRIES TO:**

Strategic Planning Group, Information Technology Services Division, (360) 438-4785.

**APPROVED**  
**Executive Ethics Board**

Date: 5/9/03