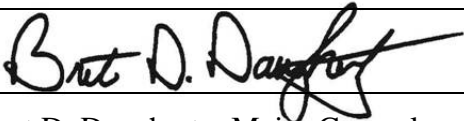




Department Policy No. IT-306-05

Title:	Use of State Provided IT Hardware and Software Resources
Former Number:	05-004-05
Authorizing Source:	RCW 42.52 Ethics in public service RCW 49.60 Discrimination - human rights commission WAC 292-110-010 Use of state resources State Technology Manual (Policies and Standards) http://ofm.wa.gov/ocio/policies/manual.asp Washington Military Department Policies: HR-207-03 ; DIR-005-08 ; and 11-01
Information Contact:	Chief Information Officer Building #20B (253) 512-7575
Effective Date:	March 23, 2012
Mandatory Review Date:	October 1, 2019
Revised:	October 1, 2015
Approved By:	 Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

Purpose

Establish the Washington Military Department (WMD) policy regarding employee use of State provided IT hardware and software resources that 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.

Additional Guidance

All electronically stored information (ESI), including but not limited to, Microsoft Office products, databases, voice mail messages, email messages, text messages, instant messaging, video chat, social media sites, and Internet usage histories are public records and subject to public records disclosure or legal discovery unless privileged or specifically exempted by law. All ESI shall be retained according to records retention requirements specified under the State Government Records Retention Schedule and

Military Department Records Retention Schedule. [The Executive Ethics Board](#) web site contains additional information and guidance related to the appropriate use of state resources.

Scope

This policy applies to all WMD employees, contractors, vendors, and business partners who have access to WMD State provided IT hardware and software resources.

Policy

A. Responsibility

1. The Network Manager:
 - a. Ensures appropriate scanning and monitoring tools, automated and manual, are employed on information systems to assess and monitor exploitable vulnerabilities and insure policy adherence.
 - b. Reviews real-time and periodic audit logs including application & security logs along with web browsing history.
 - c. Coordinates with other WMD sections to ensure that this policy is implemented effectively.
2. The IT Operations Manager:
 - a. Ensures the implementation and enforcement of this policy.
 - b. Manages and implements technologies that support the accepted WMD secure communication standards.
 - c. Periodically reviews logging records to maintain compliance.
 - d. Reports the suspected intrusion, suspicious activity or unexplained erratic behavior to the employee's Division Director and the WMD Chief Information Officer (CIO).
 - e. Collaborates with the Chief Information Security Officer (CISO) to ensure a comprehensive solution or planned course of action is implemented expeditiously.
3. The Division Director:
 - a. Reviews the content of this policy and explains its importance of protecting the integrity of WMD computing infrastructure with their staff.
 - b. Ensures new employees receive an overview of this policy prior to using the WMD computing infrastructure, computers, networks, and computer systems.
 - c. Reviews and recommends approval for exceptions to this policy.
 - d. Communicates all requests for exceptions to this policy to the CIO.
 - e. Considers these questions before recommending approval for an exception to policy:

- 1) Is the requested exception really needed to perform the work of the agency?
- 2) What risks would this exception create for the agency, the employee and yourself?
- 3) What is the estimated impact on the WMD technology environment from this exception?
- 4) What will it cost to implement and provide on-going support for this exception?
- 5) Does the budget accommodate the costs for this exception?
- 6) What security risks does this exception generate?

4. Supervisors and Employees:

- a. Each employee and contractor is responsible for the appropriate use of State provided IT hardware and software resources.
- b. Supervisors are accountable for their employee's appropriate use of State provided IT hardware and software resources.
- c. Anyone observing prohibited use of State provided IT hardware and software resources must report it to their supervisor or Division Director so that corrective and preventative action can be taken.
- d. All Supervisors are required to report any inappropriate use of computers to their Division Director and Human Resources Director to ensure consistent application of disciplinary/corrective action and prevention strategy.

B. Lack of Privacy

The WMD Director or designee may access employees' ESI without prior notification when it is necessary to carry out normal business functions, or if the Director has reason to believe misuse has occurred. If an employee has used personally-owned systems or devices to do WMD 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.

WMD may, at its discretion, filter email or Internet content without notice to employees to protect the integrity and security of all WMD State provided IT hardware and software resources.

All call records, documents and data, photos, etc. used to conduct state business, and made via personally-owned devices, are subject to records retention requirements and public records disclosure. Personal call records and other information (e.g. personal data, photos, text messages, etc.) may be subject to review or audit in the event of a litigation hold or public disclosure request. The owner of a personal cellular device may be required to surrender the device, including all personal and business related information, if it is subject to a public records request or litigation hold.

C. Employee Use of State provided IT hardware and software resources.

1. **Permitted Business Use** - Employees may use WMD provided hardware and software resources for conducting business that is reasonably related to official state duties, to include electronic recruiting and Employee Self Service.

Employees represent the WMD when using State provided IT hardware and software resources to conduct state business and are required to use these tools in compliance with State Ethics laws and standards.

2. **Permitted Personal Use** – Personal use of State provided IT hardware and software resources must comply with [WAC 292-110-010](#), which states that employees may make occasional and limited personal use of state resources 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;
 - e. The use does not compromise the security or integrity of state information or software; and
 - f. The use is not a prohibited use under C.3. below.

Prior to engaging in limited personal use of state resources, employees are encouraged to seek guidance from their supervisor as to whether the intended usage is considered to be de minimis.

3. **Prohibited Uses** – Employees are prohibited from using state-provided IT hardware and software resources in any of the following ways:
 - a. Personal use of state-provided IT hardware and software resources that does not meet the conditions found in C.2.a-f above is prohibited.
 - b. Employees must not save or store Internet browser favorites that are personal in nature. Only work related favorites are allowed to be saved on state-provided equipment.
 - c. Employees must not use state-provided email, voice mail, copying, imaging, or Internet access for conducting an outside business, private employment or activities for private financial benefit or gain.
 - d. Employees must not use state-provided email, voice mail, copying, imaging, or Internet access to conduct activities that support outside employment, to include federal National Guard and State Guard activities not within their scope of employment.

- e. Employees must not connect personally owned devices to the state-provided IT hardware and software resources provided throughout the buildings on Camp Murray. Access to State provided IT hardware and software resources is available for WMD customers and or stakeholders who are here to conduct WMD business only.
- f. Employees must not use state-provided IT hardware and software resources 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 have prior written permission from their supervisor authorizing such use.
- g. WMD employees must not use state-provided IT hardware and software resources to create, transmit, or store ESI containing or promoting:
 - 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;
 - 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; and
 - 7) Any activity that is prohibited by federal, state, or local law, or department policy.
- h. In addition, employees may not use state-provided IT hardware and software resources, to:
 - 1) Order or sell items on the Internet, except as specifically approved by the WMD for business purposes;
 - 2) Participate in any online game, contest, promotion, or sweepstakes;
 - 3) Participate in non-work related text messaging, Instant Messaging, chat groups, listservs, blogs, newsgroups or other forms of social media sites;
 - 4) Gamble;
 - 5) Solicit money or support for, or otherwise support or promote, religious or political causes, private business, or non-WMD authorized activities and events;
 - 6) Create, post, transmit, connect to, or voluntarily receive offensive, libelous, threatening, or harassing material (except as related to official

WMD authorized activities);

- 7) Link WMD web sites to other Internet sites in violation of this policy;
- 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 WMD information over the Internet; or
- 10) Tamper with or alter the configuration or settings of the agency-supplied computing device issued to them without the permission and assistance of the WMD Helpdesk.
 - i. Employees must not use state provided electronic messaging systems and devices to make requests for disclosure of public records for the personal use or benefit of themselves or others.
 - j. Employees must not establish an Internet connection (e.g., AOL, MSN, etc.) to or from a computer connected to the WMD network that bypasses the Washington State Department of Consolidated Technology Services (CTS) firewall.
 - k. Checking personal and/or outside non-WMD email accounts using WMD computers, and/or the State Government Network is prohibited. Employees must not use email products on WMD computers other than those provided and supported by the WMD. Some examples of prohibited products include email accounts offered by Hotmail, Yahoo, EarthLink, MSN, Comcast and AOL.
 - l. Using text or instant messaging offered by an external vendor that is not provided and supported by the WMD is prohibited.
 - m. Employees must not create, forward, or store ESI that does 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.
 - n. Employees who are on the WMD 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 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 WMD’s Wide Area Network.
 - o. Employees must not download or install any software without the consultation, guidance and approval from the Information Technology Division.
 - p. While using the Internet, if at any time an employee inadvertently accesses an inappropriate site, the employee should immediately close

the page and notify his or her supervisor.

D. 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 or sexually explicit Materials: The WMD has a zero tolerance regarding pornographic or sexually explicit materials in the workplace. If, after an investigation, it is found that an employee used state resources to create, access, post, transmit, print, or store pornographic or sexually explicit materials that are inappropriate for the workplace, appropriate disciplinary action will be taken up to and including termination from WMD employment. The Division Director will consult with the Adjutant General and Human Resources to determine the level of disciplinary action taken.
3. If a contractor used state resources to create, access, post, transmit, print, or store pornographic or sexually explicit materials, the WMD will take appropriate action as provided in the contract.

E. Examples of Permitted and Prohibited Use

Example 1: An employee makes a local telephone call or sends an email communication to his or her home to make sure his or her children have arrived home safely from school. This is not a violation of this policy.

- 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 violation of this policy.

- 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: Two or three times a month an employee quickly uses the Internet to check his or her children's school web site to confirm if school will end early that day. Each transaction takes two to three 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 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.

Such actions are not violations of the policy 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 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 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 VIOLATION OF THIS POLICY.*

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 VIOLATION OF THIS POLICY.*

- 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, which can compromise state databases.

Frequently Asked Questions

Question:	Can I check my personal email account from my agency-supplied computer?
Answer:	No, this is prohibited use and would pose a security risk to the agency.
Question:	Can I install a game to use during my breaks or to entertain my child when they are at work with me?
Answer:	No, this is a prohibited use and would pose a security risk to the agency.
Question:	Can I use my agency-supplied computer to access CNN.com to check national news?
Answer:	Yes, if it falls within the de minimis use provision of the ethics policy or if such access is a required part of your official duties or responsibilities.
Question:	Can I install a cool screen saver I saw on the web?
Answer:	No, this is prohibited use and would pose a security risk to the agency.
Question:	Can I receive and send email to family and friends on a regular basis? Is there a reasonable time limitation here?
Answer:	No, regular is not infrequent and fails the de minimis use test outlined in the ethics policy.
Question:	Can I use my agency-supplied computer to check my state deferred compensation or state retirement accounts?
Answer:	Yes, this is within the de minimis use test outlined in the ethics policy and both retirement and deferred compensation are part of state employees benefit package.
Question:	Can I download software if it enables me to do my job better?
Answer:	No, this would pose a security risk to the agency. However, you can submit a request through your supervisor to the WMD Help Desk to assess the software you are interested in. It will be up to the Chief Information Officer to grant an exception to this policy.
Question:	Can I use my agency-supplied computer to listen to web radio?
Answer:	No, this consumes network resources and is not de minimis.
Question:	Can I download music from the Internet and listen to it?
Answer:	No, since there are many issues with ownership of downloaded music, you cannot put the agency at risk. You can listen to music on CDs as long as it meets the de minimis use test outlined in the ethics policy, and does not interfere with co-workers.
Question:	Can I bring in my personal laptop and use the agency network to get security updates?
Answer:	No, connecting any unauthorized computer to the WMD network is not allowable for any reason.

Definitions

Blog (abbreviation for web log): A web site where entries are written in chronological order and commonly displayed in reverse chronological order. Many blogs provide commentary or news on a particular subject; others function as more personal on-line diaries allowing readers to leave comments in an interactive format.

Chat Group: A service offered through a Web site, or part of a site, or part of an Internet connection service, such as America Online, that provides a venue for communities of users to communicate in real time, usually focused on a common interest.

Confidential Information: Information that is protected by state or federal laws including information about the WMD's clients, employees, vendors or contractors, and agency systems.

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.

Electronically Stored Information (ESI): Computer data or electronic recorded media of any kind that is stored in a digital medium from which it can be retrieved and examined. ESI includes but is not limited to e-mail, Microsoft Office products, text messaging, instant messaging voice mail, video chat, databases, social media sites or any other software. ESI can be located on network servers, backup tapes, thumb drives, CDs, DVDs, floppy disks, work computers, cell phones, laptops or any other electronic device including department information created by agency employees using personal electronic devices.

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 agency 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.

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. Two of the most popular mailing list server systems for the Internet are Listserv and Majordomo.

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's or employee's agency or by statute or the state Constitution. ([RCW 42.52.010](#))

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 to primarily arouse sexual desire or cause sexual arousal.

Social Media or Social Networking: Interaction with external internet websites or services based on participant contributions to the content. Types of social media may include blogs, micro blogs, social and professional networks, video or photo sharing, and social bookmarking. Examples of social media sites are *YouTube, Facebook, Flickr, Twitter, WordPress, MySpace, RSS, Second Life, LinkedIn, Delicious*, etc.

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.