

PERSONAL COMPUTER USAGE POLICY

IS Team Approval: Unanimous w/3 Absent, February 16, 2006

TAB Review Date: February 21, 2006

TAB Approval Date: March 20, 2006, Unanimous

Director Approval Date: March 22, 2006

OSF Specification:

5.3—Personal Computer Usage

The agency computers of the State are provided for job related activities. To this end, the hosting agency provides support in networking and information resources for its computing community.

All users are given access to computers for job related duties and this usage **must** remain in compliance with State and agency policies as well as all state and federal laws governing usage and communication of information. Failure to comply will result in the denial of access privileges and may for employees lead to disciplinary action up to and including dismissal. For contractors, it may lead to the cancellation of the contractual agreement. Litigation may ensue.

In the effort to protect the integrity of the statewide network and its systems, any proof of unauthorized or illegal use of any agency computer and/or its accounts will warrant the immediate access to these files, accounts and/or systems by the hosting agency's security and information systems staff and appropriate action will be taken.

Information Security Policy for computer usage prohibits the use of its resources to:

- A. Send email using someone else's identity (Email forgery).
- B. Take any action that knowingly will interfere with the normal operation of the network, its systems, peripherals and/or access to external networks.
- C. Install any system or software on the network without prior approval.
- D. Install any software systems or hardware that will knowingly install a virus, Trojan horse, worm or any other known or unknown destructive mechanism.
- E. Attempt IP spoofing.
- F. Attempt the unauthorized downloading, posting or dissemination of copyrighted materials.
- G. Attempt any unauthorized downloading of software from the Internet.
- H. Transmit personal comments or statements in a manner that may be mistaken as the position of the State.
- I. Access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age, disability, medical condition, sexual orientation or any other status protected by state and federal laws.

Furthermore, it is the State's position that all messages sent and received, including personal messages and all information stored on the agency's electronic mail system, voicemail system or computer systems are State property regardless of the content. As such, the hosting agency reserves the right to access, inspect and monitor the usage of all of its technology resources including any files or messages stored on those resources at any time, in its sole discretion, in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information or for any other business purpose.

ODCTE Implementation:

5.3 Personal Computer Usage

The ODCTE computers are provided for job related activities. All users are given access to computers for job related duties and this usage must remain in compliance with State and ODCTE policies as well as all state and federal laws governing the usage and communication of information.

In the effort to protect the integrity of the ODCTE network and its systems, the agency prohibits the use of its resources to:

- A. Use someone else's identity to send email or gain access to network resources.
- B. Take any action that will interfere with the normal operation of the internal or external network.
- C. Install any hardware or software on the ODCTE network, its servers, or workstations without prior approval from SDCS. This includes but is not limited to:
 1. Hardware
 - a. Switches
 - b. Hubs
 - c. Wireless access points (WAPs)
 2. Software
 - a. I-news
 - b. Weather tracking
 - c. File sharing
 - d. Music sharing
 - e. Online radio
 - f. Games
 - g. Browser plug-ins and tool bars

- D. Install any software systems or hardware that will propagate a virus, Trojan horse, worm, or any other destructive mechanism.
- E. Spoof IP or MAC addresses.
- F. Upload, download, or distribute pirated software or data.
- G. Transmit personal comments or statements in a manner that may be mistaken as the position of the ODCTE or State.
- H. Access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age, disability, medical condition, sexual orientation or any other status protected by state and federal laws.

All information installed and stored on agency computer systems and media is ODCTE property regardless of the content. The ODCTE reserves the right to access, inspect, and monitor the usage of all of its technology resources to determine compliance.

Failure to comply with any of these policies may result in the denial of access privileges and may be reported to proper management. For contractors, it may lead to the cancellation of the contractual agreement.

For assistance with this policy, please contact Computer Support.