



State of Oklahoma
Oklahoma Department of Agriculture, Food, and Forestry

Policies and Procedures
Electronic Devices

Effective Date of Policy: 11/1/2014	Next Scheduled Review:
Prior Policy Number:	Policy Number: ODAFF-06
Last Reviewed:	Replaces Policy Number:
Date Policy Last Revised:	
Approved: Jim Reese	Approval Date: 10/1/14

Reference: *State Security Policy (2003)*

A. Electronic Devices

ODAFF computers, cellular telephones, or other electronic devices may be provided to employees for job-related activities. Employees using electronic devices for job-related duties and this usage must be in compliance with state and agency policies as well as all state and federal laws governing usage and communication of information. While on duty employees shall always devote full time, attention and effort to the duties and responsibilities of their positions. The use of ODAFF electronic devices shall be job related, professional in nature, and comply with all applicable state and agency policies.

ODAFF electronic devices are ODAFF property and should not be used for personal purposes even if the employee is "off the clock." All data stored on ODAFF computers, cellular telephones, or related servers, including but not limited to, browser histories, emails, voicemails, and texts are the property of ODAFF. Accordingly, employees should have no expectation of privacy concerning such data. ODAFF personnel, including supervisors and division directors, may access ODAFF data without seeking permission from the employee. Further, such data may be produced in response to a valid open records request unless specifically exempted from disclosure by law.

B. State Security Policy

The State Security and ODAFF policy for computer usage prohibits the use of its resources to send email using someone else's identity (e-mail forgery); take any action that knowingly will interfere with the normal operation of the network, its systems, peripherals and access to external networks; install any system or software on the network without prior approval; install any software systems or hardware that will knowingly install a virus, trojan horse, worm or any other known or unknown destructive mechanism; attempt IP spoofing; attempt the unauthorized downloading, posting or dissemination of copyrighted materials; attempt any unauthorized downloading of software from the Internet; transmit personal comments or statements in a manner that may be mistaken as the position of the state; or 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.

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 or its accounts will warrant the immediate access to these files, accounts or systems by the hosting agency's security and information systems staff and appropriate action will be taken.

Furthermore, 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.

State Security Policy (2003)

C. Enforcement

Employees who violate this policy are subject to discipline, up to and including termination. For contractors, it may lead to the cancellation of the contractual agreement.