State of Oklahoma
A Division of the Office of Management and Enterprise Services
Policies and Procedures
Computer and Mobile Computing Device Usage

Effective Date of Policy: 04/16/2018	**Next Scheduled Review: 03/01/2020**
Effective Date of Original Policy: 01/01/2013	**Policy Number: OMES-20**
Last Reviewed: 03/07/2018	**Replaces Policy Number: HCM - 06**
Date Policy Last Revised: 03/07/2018	
Approved: Denise Northrup, OMES Director	**Approval Date: 04/03/2018**

Reference
The State Security Policy

Policy
The agency computers and mobile computing devices, including but not limited to cell phones, laptop computers and tablets, of the State are provided for job-related activities. To this end, the Office of Management and Enterprise Services (OMES) provides support in networking and information resources for its computing community. All users are given access to computers, and mobile computing devices as necessary, 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. While on duty, employees are to always devote full time, attention and effort to the duties and responsibilities of their positions.

Procedure
The State Security Policy and OMES policy for computer usage prohibits the use of its resources to:

1. Send email using someone else's identity (e-mail forgery).
2. Take any action that knowingly will interfere with the normal operation of the network, its systems, peripherals and/or access to external networks.
3. Install any system or software on the network without prior approval.
4. Install any software systems or hardware that will knowingly install a virus, Trojan horse, worm or any other known or unknown destructive mechanism.
5. Attempt IP spoofing.

6. Attempt the unauthorized downloading, posting or dissemination of copyrighted materials.
7. Attempt any unauthorized downloading of software from the Internet.
8. Transmit personal comments or statements in a manner that may be mistaken as the position of the state, and
9. 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 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.

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.

Failure to comply will result in the denial of access privileges and may for employees lead to disciplinary action up to and including termination of employment. For contractors, it may lead to the cancellation of the contractual agreement. Litigation may ensue.

The State Security Policy is located here: http://www.ok.gov/cio/documents/InfoSecPPG.pdf