

# **Social Networking and Social Media Policy**

## **State Policy and Standard Specification**

The Commissioners of the Land Office (CLO) adheres to the State of Oklahoma Social Networking and Social Media (SNSM) policies at

- [http://www.ok.gov/cio/Policy\\_and\\_Standards/Social\\_Media/](http://www.ok.gov/cio/Policy_and_Standards/Social_Media/)

which include:

1. State of Oklahoma Social Networking and Social Media
2. State of Oklahoma Social Networking and Social Media Development Methodology
3. State of Oklahoma Social Networking and Social Media Guidelines

CLO employees using SNSM services for official agency business shall adhere to State of Oklahoma SNSM technology toolkits, when published by the Office of Management and Enterprise Services (OMES).

### **Other Applicable State of Oklahoma Standards**

All Web 2.0 and SNSM technologies shall also adhere to the following:

- [State of Oklahoma Information Technology Accessibility Standards](#)
- [Oklahoma Information Security Policy, Procedures, and Guidelines](#)

### **Implementation**

The CLO recognizes the potential benefits of a SNSM presence to disseminate public information about the CLO's mission, goals, and accomplishments. During regular work hours or using CLO equipment, CLO employees shall only use SNSM services to conduct official agency business. The Communications Director shall enforce applicable SNSM policies and refer CLO employees engaging in the inappropriate use of SNSM technologies to the employee's supervisor for appropriate disciplinary action.

### **Use**

Only the Communications Director or approved CLO employees shall use SNSM sites to conduct official agency business, as follows:

- A. The Communications Director shall oversee and manage official SNSM accounts and content.
- B. CLO employees must have written authorization from the Communications Director to publish content on official SNSM accounts.
- C. Approved CLO employees shall use non-administrative login accounts and designated workstations to publish official content to an OMES-approved SNSM provider.
- D. The Communications Director shall maintain a log detailing authorized SNSM service providers, current account names, master passwords, and CLO employees authorized to use official SNSM accounts.

The CLO and its employees shall observe and comply with the following policies concerning SNSM content and use:

- A. All state and agency policies and guidelines pertaining to e-mail shall also apply to SNSM content, including, but not limited to policies regarding solicitation, obscenity, harassment, pornography, sensitive information, and malware.
- B. Official SNSM content reflect the CLO. Usernames, comments, photos, videos, etc., shall be appropriate for a professional environment and selected in good taste.
- C. Official content posted on SNSM sites shall comply with the State of Oklahoma Information Security Policy, Procedures and Guidelines.
- D. The CLO shall respect copyright laws and reference sources appropriately. The CLO and its employees shall identify any copyrighted or borrowed material with citations and links.
- E. The CLO shall not disclose confidential or proprietary information of employees or persons doing business with the CLO in any form of online media.
- F. The CLO recognizes that SNSM content is public and employees shall be responsible for official SNSM content.
- G. CLO employees shall disclose affiliation with the CLO and shall respect the privacy of colleagues and the opinions of others.
- H. CLO employees shall avoid personal attacks, online fights, and hostile personalities.
- I. The CLO shall ensure official SNSM content is accurate and truthful.
- J. The CLO shall ensure SNSM content and comments comply with the Commenting Policy, found in the State of Oklahoma Social Networking and Social Media Policy and Standards.
- K. The CLO and its employees shall not post SNSM content that could:
  - a. compromise the safety or security of the public or public systems,
  - b. compromise solicitations of commerce,
  - c. promote or oppose any person campaigning for election to a political office,
  - d. promote or oppose any ballot proposition, or
  - e. promote, foster, or perpetuate discrimination on the basis of race, creed, color, age, religion, gender, marital status, national origin, physical or mental disability, or sexual orientation.
- L. Online activity that may violate applicable local, state, or federal laws or regulations is prohibited.

### **Security**

SNSM content has the potential to compromise the security of CLO computer systems. Most SNSM traffic is sent in clear text that is not encrypted. The CLO and its employees shall observe and comply with the following SNSM security policies:

- A. A SNSM service provider and associated plug-ins shall be selected from the applicable sections, policies and standards set forth on the [OMES Social Media page](#).
- B. To maintain security of the CLO network usernames and passwords, a SNSM user must use a unique username/password combination that differs from his or her login ID and password for the CLO network.

- C. Sensitive information such as usernames, passwords, social security numbers and account numbers passed via SNSM can be read by parties other than the intended recipient(s). Transferring sensitive information over SNSM is prohibited.
- D. Peer-to-peer file sharing is not allowed through the CLO network. SNSM clients are prohibited from using peer-to-peer file sharing.
- E. Many SNSM clients provide file transfers. Policies and guidelines pertaining to e-mail attachments also apply to file transfer via SNSM.
- F. SNSM can make a user's computer vulnerable to compromise. A SNSM user should configure his or her SNSM account(s) in such a way that messages are not received from unauthorized users.

### **Ethics and Code of Conduct**

As a state employee Web 2.0 and SNSM technologies are governed by the prevailing ethics rules and statutes. In addition, all assigned Web 2.0 and SNSM duties are governed by the Oklahoma State Constitution, Oklahoma statutes and applicable rules, and the CLO computer usage policies.

### **Records Management and Open Records**

All SNSM communications are subject to the requirements of the Office of Records Management and the Child Internet Protection Act (CIPA). [Information about this act and its requirements](#) is found on the Federal Communications Commission (FCC) website

All content, comments, and replies posted on any official OMES Web 2.0 or SNSM technology are subject to the Oklahoma Open Records Act. Information disseminated using SNSM technology is subject to being re-printed in newspapers, magazines, or online in another online media format. Official SNSM content created or received by CLO personnel meeting the definition of a "record" shall be retained as required by law.

### **Monitoring**

SNSM traffic shall be logged and reviewed. Logging activity may help in the event a CLO account is compromised or improper information is posted.

Logging shall include the following information:

- Name of user
- Date/Time of use
- User's activity

CLO employees shall have no expectation of privacy when using CLO equipment. Supervisors may request or be provided reports of Internet usage by the CLO information security officer or state chief security officer. Any CLO employee misusing an SNSM service or violating the CLO policy on such SNSM use may be disciplined, up to and including termination.

### **Communication**

The CLO may use SNSM accounts to communicate with media, other agencies, and the general public in times of crisis, emergency, or disaster.