Policies and Procedures

Social Networking and Social Media

Effective Date of Policy:	Next Scheduled Review: 1-2-2022
Last Reviewed:	Policy Number: OCC-14 (2021)
Date Policy Last Revised:	Replaces Policy Number:
Approved:	Approval Date:

Reference: *74 O.S. § 840-8.1*

A. State Policy and Standard Specification

The Commission adheres to the *State of Oklahoma Social Networking and Social Media (SNSM) policies* 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

All Commission activity on SNSM platforms Twill adhere to State of Oklahoma SNSM technology toolkits.

Other Applicable State of Oklahoma Standards

All Web 2.0 (Web 2.0 refers to websites that emphasize user-generated content, ease of use, participatory culture and interoperability for end users) and SNSM technologies shall also adhere to the following:

- State of Oklahoma Information Technology Accessibility Standards
- Oklahoma Information Security Policy, Procedures, and Guidelines

B. Implementation

To protect the position, image and information assets of the Commission, the use of SNSM services is intended for agency purposes only. The Commission recognizes the potential marketing benefits of a SNSM presence and its use is meant to promote and market the mission and goals of the Commission and its conservation partners.

Agency employees that are approved to administer the Commission's SNSM platforms are prohibited from using personal accounts for any state agency related business on any SNSM site. The approved agency employee and the division/business unit manager are to follow all applicable policies and implementation guidelines, and bear the responsibility for any issues caused by an approved employee engaging in the inappropriate use of SNSM technologies.

C. Use

The Executive Director shall designate a Communications Director that shall be responsible for overseeing the Commission's brand identity and key messages communicated on the SNSM sites. The Communication Director will maintain a log of all SNSM services used by agency employees in the course of official business.

1. The Communication Director is responsible for oversight and management of all agency accounts with SNSM providers.
2. Authorization for the engagement with agency SNSM accounts is a function of the Communications Director. Written approval from the Communications Director is required prior to compilation and publishing using these accounts.
3. The Communications Director will provide the Executive Director with documentation detailing the authorized SNSM service providers, the current account names, the master passwords and person(s) authorized to use the accounts.

   The following statements also apply to SNSM usage:

   a. All state and agency policies and guidelines pertaining to e-mail also apply to SNSM, including, but not exclusive to, policies regarding solicitation, obscenity, harassment, pornography, sensitive information, and malware.
   b. Commission SNSM sites should reflect the agency's name. Usernames, comments, photos, videos, etc., should be appropriate for a professional environment and selected in good taste.
   c. Information published on SNSM sites should comply with the State of Oklahoma Information Security Policy, Procedures, and Guidelines.
   d. Respect copyright laws and reference sources appropriately. Identify any copyrighted or borrowed material with citations and links.
   e. It is inappropriate to disclose or use the Commission's, an employee's, or a respective client's confidential or proprietary information in any form of online media.
   f. When representing the Commission in any SNSM activity, the approved employee should be aware that all actions are public and the employee(s) will be held fully responsible for any and all online activities.
   g. An approved employee must disclose that he or she is affiliated with the Oklahoma Conservation Commission and must respect the privacy of colleagues and the opinions of others.
   h. Avoid personal attacks, online fights, and hostile personalities.
   i. Ensure material is accurate, truthful, and without error.
   j. The Commission will ensure comments comply with the Commenting Policy, found in the State of Oklahoma Social Networking and Social Media Policy and Standards.
   k. Content that could compromise the safety or security of the public or public systems, solicitations of commerce, or promotion or opposition of any person campaigning for election to a political office or promoting or opposing any ballot proposition shall not be posted to SNSM sites. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, with regard to public assistance, national origin, physical or mental disability, or sexual orientation shall not be posted to SNSM sites.
   l. Do not conduct any online activity that may violate applicable local, state or federal laws or regulations.

D. Security

SNSM has the potential for security-related issues. Most SNSM traffic is sent in clear text that is not encrypted. The following statements apply to SNSM security:

1. 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.*
2. To maintain security of the Commission's 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 Commission network.
3. 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.
4. Peer-to-peer file sharing is not allowed through the Commission network. SNSM clients are prohibited from use of peer-to-peer file sharing.
5. Many SNSM clients provide file transfers. Policies and guidelines pertaining to e-mail attachments also apply to file transfer via SNSM.
6. 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.

E. Escalation

In the event a virus, malware, or any other suspicious activity is observed on the user's machine, a user shall immediately contact the OMES Service Desk for prompt assistance to determine the cause of the situation.

F. 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 Commission computer usage policies.

G. 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 can be 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 any other online media format.

Social computing content created or received by state agency personnel may meet the definition of a "record" as defined by state statute, when the content is made or received in connection with the transaction of the official business of the agency, and should be retained as required. This applies

to content made or received whether during work hours or on personal time regardless of whether the communication device is publicly or privately owned.

H. Monitoring

SNSM traffic is logged and reviewed. Logging activity may help in the event an agency account is compromised or improper information is posted to the agency SNSM account.

Logging should at a minimum include the following information:

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

Users should have no expectation of privacy. Supervisors may request or be provided reports of Internet usage by employees from the agency information security officer or state chief security officer, as applicable, as needed to monitor use.

Any employee found to have misused or abused a SNSM service or violated this policy may be subject to disciplinary action, up to and including termination of employment.

I. Communication

The Commission will use SNSM as another tool to connect with media, other agencies, and the general public.

The Commission may also use SNSM in times of crisis and to assist with emergency, disaster or crisis communications. Information to be published on the agency SNSM sites during times of crisis shall need to be deemed applicable and prudent by the Oklahoma Conservation Commission Executive Director.