State of Oklahoma
Office of Management and Enterprise Services
Policies and Procedures

Social Networking and Social Media Policy

Effective Date of Policy: 03/17/2015	**Next Scheduled Review: 01/02/2016**
Prior Policy: NA	**Policy Number: OMES-006**
Last Reviewed: 02/19/2015	**Replaces Policy Number: NA**
Date Policy Last Revised: 02/19/2015	
Approved: Lucinda Meltabarger, as designee of Dir. Preston L. Doerflinger	**Approval Date: 03/17/2015**

Purpose

The Office of Management and Enterprise Services (OMES) adheres to the State of Oklahoma Social Networking and Social Media (SNSM) policies found at 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

Approved agency employees using SNSM during the course of agency business and approved agency employees representing the agency on social media in the normal course of business, shall adhere to State of Oklahoma SNSM technology toolkits, when published by OMES.

This policy governs the use of social networking and social media technologies for business purposes by OMES, including defining oversight, acceptable business and personal use, and establishing operational policy. OMES SNSM technology is intended for interaction with the public through external communication.

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

Definitions

The words and terms included in this policy follow the State of Oklahoma SNSM Policy and Standards and shall have the same meaning unless the context clearly indicates otherwise.

Scope

OMES endorses the secure use of SNSM to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity improvement.

A. When SNSM sites are accessed, OMES employees are subject to all governing statutes and policies including, but not limited to:
    a. 74 O.S. § 840-2.11 regarding confidentiality of state employee personal information;
    b. 74 O.S. § 1322 regarding confidentiality of insurance files;
    c. 40 O.S. § 173.2 regarding limitations on employer access to online social media accounts of employees
    d. Information security;
    e. Disciplinary action;
    f. Fair Labor Standards Act;
    g. Code of Ethics;
    h. Anti-Harassment;
    i. Anti-Violence, Bullying, Workplace Violence;
    j. Computer Usage;
    k. Health Insurance Portability and Accountability Act (HIPAA);
    l. records retention rules; and
    m. OMES social networking and social media standards per http://www.ok.gov/cio/Policy_and_Standards/Social_Media/.
B. Inappropriate use of SNSM by OMES employees may be grounds for disciplinary action per the OMES Computer Usage policy. Further, when SNSM is used for official agency business, the SNSM is subject to OMES policy.

Oversight

The OMES director designates the OMES communications and public affairs directors as responsible for oversight of OMES's brand identity and key messages communicated on OMES SNSM sites. OMES Public Affairs shall maintain a log of all SNSM services used by agency employees in the course of official business.

A. OMES Public Affairs is responsible for oversight and management of all agency accounts with approved SNSM providers.

B. Authorization for the engagement with agency SNSM accounts is a function of OMES Public Affairs. Written approval from OMES Public Affairs is required prior to compilation and publishing using these accounts.

C. Approved OMES employees, who have obtained written permission from OMES Public Affairs, must use non-administrative login accounts; and designated workstations should be used to publish content to an OMES-approved SNSM provider.

D. OMES Public Affairs shall provide the OMES information security officer with documentation detailing the authorized SNSM service providers, the current account names, the master passwords and person(s) approved to use the accounts.

OMES Implementation

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

Approved OMES employees are prohibited from using personal accounts for any state OMES-related business on any SNSM site. Approved OMES employee(s) and the division/business unit manager(s) 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. OMES shall only implement SNSM technologies included on the approved list of SNSM technologies found on the OMES CIO website.

Business Use of SNSM by OMES Employees

Approved OMES employees and divisions may use SNSM to officially interact with citizens, and stakeholders, but only with prior written authorization from OMES Public Affairs.

A. To obtain authorization from OMES Public Affairs, there must be:
    a. verification the technology is on the statewide list of approved technologies;
    b. an identified employee to moderate comments, if commenting features are enabled, as part of his or her accountabilities listed on OPM-111;
    c. approval by the respective OMES division director/administrator for a designated employee to use the SNSM technology; and
    d. completion of an SNSM employee education course provided by OMES Public Affairs that covers:
        i. Terms of use restrictions

ii. Legal issues
iii. Policy
iv. SNSM best practices, etiquette and "norms"
v. Security

B. Once OMES Public Affairs approves the use of SNSM:
    a. division staff ensures the site is monitored, assuring compliance with state law and OMES policy; and
    b. OMES Public Affairs reviews the SNSM content prior to posting and reserves the right to restrict or remove any content deemed in violation of OMES standards or applicable laws.
C. OMES-related communication through SNSM is professional in nature and always conducted per OMES policy, practices and expectations. Employees must be respectful and thoughtful in the business use of SNSM and must adhere to the State of Oklahoma Commenting Policy.

Use

The following statements also apply to SNSM usage:

A. All state policies and guidelines pertaining to email also apply to SNSM, including, but not exclusive to, policies regarding solicitation, obscenity, harassment, pornography, sensitive information, HIPAA and malware.
B. Agency SNSM sites reflect the OMES brand. Usernames, comments, photos, videos, etc., should be appropriate for a professional environment and selected in good taste. The OMES public affairs director shall approve/disapprove all questionable content.
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. If a site requires permission in order to use its content, submit an OMES Copyright Approval Form with OMES Public Affairs.
E. It is inappropriate to disclose or use OMES's, an employee's or a respective user's confidential or proprietary information in any form of online media.
F. When representing OMES in any SNSM activity, the approved employee should be aware that all actions are public and the employee(s) shall be held fully responsible for any and all said activities.
G. A approved employee(s) must disclose that he or she is affiliated with OMES 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 and truthful.
J. OMES shall ensure comments comply with the State of Oklahoma Commenting Policy.
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.

Crisis Communication

OMES shall use SNSM as another tool to connect with media, other agencies and the general public in times of crisis and to assist with emergency, disaster or crisis communications. Information to be published on the agency SNSM sites may include potential delays or closures of sites or services as deemed applicable and prudent by the OMES director.

Important crisis management planning steps:

A. Establish notification and monitoring systems; use your website to communicate
B. Remove marketing that is unhelpful to your plight
C. Connect directly with your audience
D. Be easily visible on social media
E. Identify a crisis communication team; appoint a spokesperson

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:

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 OMES 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 OMES 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 OMES network. SNSM clients are prohibited from use of 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 unapproved users.

Escalation

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

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 OMES 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 available 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.

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. Each OMES division/business unit is responsible for logging this information and submitting a monthly report to OMES Public Affairs.

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. The OMES director, or a designee, shall be provided access to a list of the agency users for SNSM, upon request.

Personal Use of SNSM by OMES Employees

OMES employees may use personal SNSM.

A. Guidelines for SNSM use are as follows.
    a. SNSM is not allowed on agency time or on agency equipment unless it is being used to conduct agency business.
    b. OMES employees exercise caution when posting to personal SNSM sites. By virtue of their position, they must consider whether published personal content may be misunderstood as expressing an official OMES position.
    c. Any SNSM use, when used on OMES equipment is subject to monitoring; the employee should have no expectation of privacy. Employees may be disciplined for unauthorized use of equipment.
    d. When posting or commenting about job functions and/or the state of Oklahoma on personal SNSM accounts, it is recommended that employees post a disclaimer as a permanent part of any personal SNSM profile, such as, "The postings on this site are my own and may not necessarily reflect or represent the opinions of my employer."
    e. Employees are responsible for all SNSM activity, including postings on the sites of others.
    f. SNSM content created or received by state agency personnel, whether during work hours or on personal time, and regardless of whether the communication device is publicly or privately owned may meet the definition of an open record 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.
B. Employees must:
    a. use a personal email address, not an OMES email address, for all personal SNSM accounts;

b. ensure personal use of SNSM, including the language and topics of comments and posts, does not interfere with work commitments and accountabilities;
c. never pretend to be someone else or use an anonymous profile when posting about job functions, OMES or State of Oklahoma business; and
d. obtain written permission from OMES Public Affairs to use the OMES logo on personal SNSM accounts.

C. Any SNSM activity by an OMES employee can become part of an official investigation.

Inappropriate or unbecoming usage of SNSM by an OMES employee may be grounds for disciplinary action up to and including termination, per OMES policy.