OKLAHOMA
Office of Management
& Enterprise Services

Social Networking and Social Media Development Methodology

Published Nov. 25, 2013
(Issued, March 2010)

Version 1.5 Issued by the Office of Management and Enterprise Services, updated 10/18/2023.

SOCIAL NETWORKING AND SOCIAL MEDIA DEVELOPMENT METHODOLOGY

Prior to using or creating a social networking, Web 2.0 or social media account or implementing any new web application tool, it is important to properly plan. The high-level development guidelines below are an example for State of Oklahoma agencies to follow.

For unapproved technologies, please be aware that the Information Services Division of the Office of Management and Enterprise Services is currently evaluating the Terms of Service/Terms of Use agreements for a number of social media, Web 2.0 and social networking technology providers, including a review of efforts undertaken by the Federal government to renegotiate agreements with a number of these providers.

Once a vendor has been approved, OMES will post the revised agreement and link to the vendor on its website, along with instructions for implementation.

1. Agency Policy

Establish a policy governing acceptable/unacceptable use of social networking, Web 2.0 or social media sites within the agency. Be sure to cover the following topics:

- Creation and maintenance of official State agency sites;
- Agency postings to non-agency sites;
- Use of agency computers to access social networking, Web 2.0 and social media sites;
- Site blocking and the use of web filtering software or firewall settings;
- Exceptions to site blocking to allow individuals access as approved;
- Review period for the policy. The policy should be reviewed annually; and
- Personal devices, Universal Serial Bus (USB) and all removable media (see Appendix A for an example of this policy)

2. Business Concept / Requirements Definition / Approval

A well thought out business case should be written to answer the following questions.

- Who: Who is initiating this request? Who is going to be creating the technology and maintaining it? Who will have approval authority over the content?

- What: What is it that you want to create? Define the scope of the project. What are the software requirements and Internet access needed to create the project? Do the Terms of Service/use violate and provisions of the State Constitution or state statute? Are any fees involved and is the money in the budget for this project? What are your strategic goals? What metrics will you capture that correspond to your goals?

- Why: Define the audience(s) focus and marketing plan for the site. This should include the overall goal of the site, page, social media, Web 2.0 or social networking technology being deployed.

- How: How often will the content be updated and posted to the site, (blog, page, or tool)? What type of content will be posted (give examples of the topics or categories of content the page, blog or tool will address)? How will approval of the content be handled? What does the approval process look like and how does it work? How will you measure the return on investment (ROI)?

3. Awareness Training

Employees with access to social networking, Web 2.0 or social media technologies need to recognize the security risks. Agencies are encouraged to provide training on a regular basis about these risks to employees before they use them for official agency business. Some of the recommended information security guidelines agencies should follow include:

- **Content**
  - Appropriate versus inappropriate
  - What content is considered confidential (HIPAA, FERPA, etc.)
- **Usage and prevention**
  - Use of state computer equipment is for official state business only.
  - For devices accessing these sites, ensure anti-virus software is current.
  - Ensure anti-spyware software is current.
  - Ensure that operating system and application patches are applied.
  - Ensure that application updates and patches are applied.
  - Ensure that users do not have "administrator privileges" on state owned computers that access the Internet.
- **URL Shortening**
  - URL shortening tools, such as tinyurl and Bit.ly, conceal the actual website link and can direct users to malicious websites.
  - Since the sunsetting of the URL shorterner provided by Go.USA.gov, there is currently no approved shortener.
  - If you determine you need a shortened URL, consider requesting a redirect URL.
- **Social Engineering/Phishing**
  - These sites are the #1 target for social engineering, phishing and malware attacks.
  - Identities are anonymous on the web; you may not be communicating with whom you think you are.

- **Passwords**
  - Never use your State agency username or password or network credentials on these sites.
  - Strong and unique passwords must be used for each individual website.
- **Privacy**
  - Confidential information should never be posted to any social networking, Web 2.0 or social media site.
  - Professional and personal content on these sites should never be mixed.
  - Don't share personal information, travel plans or information about others without their consent.
  - Enable and utilize privacy features included with the social networking, Web 2.0, or social media sites.
- **Malware**
  - Custom written video players may contain malware; think twice before you click.
  - Do not visit unknown or un-trusted websites.
  - websites can redirect and download malware to your computer if not patched.
  - Do not download files from linked websites you do not know or trust.
  - Malicious files can be in the form of commonly accepted file formats such as PDF documents, Microsoft Office products and others.
- **Reporting**
  - Work with your IT staff to ensure your computer is properly patched.
  - Always report incidents promptly to your Information Security Officer following the process in the Oklahoma Information Security Policy, Procedures and Guidelines.

4. Content Definition

Draft a sample of the type(s) of content that will be displayed using the technology and submit the sample(s) with the proposal. Also, draft a brief description on the purpose of the social networking, Web 2.0 or social media technology being deployed. Official agency postings to unofficial agency social networking, Web 2.0 or social media sites:

- Should require agency management approval;
- Should be clearly identified with the employee and agency name; and
- Should not include confidential information and should conform to the Oklahoma Information Security Policy, Procedures and Guidelines.

5. Design/Look

When applicable, OMES ISD shall define standards, including a look and feel (or template), for state agencies to use when implementing individual approved social networking, Web 2.0 or social media technologies. As these standards are developed, OMES will communicate the standards to all state agencies. In turn, all agencies are required to review this standard and make all staff members aware of their responsibility.

6. Metrics/Analytics

Establish how and what you will track in order to measure the effectiveness of your social media and social networking presence. Here are some items that you may want to consider:

- If you offer a service to your customers, you will want to measure how many of the clicks or followers translate to paying customers
- How will you measure the impact to the awareness of your agency's brand or mission?
- Can you measure if and how much the social media or social networking technology has helped reduce communications costs?
- Can you measure if and how much the social media or social networking technology has helped streamline customer relations?
- Has the social media or social networking technology has helped the agency respond more favorably to requests and/or issues?

7. Official Agency Sites

While official State agency social networking, Web 2.0 or social media technologies must meet standards detailed in the State Social Networking and Social Media Standard, agencies are encouraged to develop standards for governing their agency-sponsored social networking, Web 2.0 or social media sites. This guidance should include the following:

- Ensure the chosen technology is on the list of approved technologies.
- Agency management should approve the business concept plan, design and content for official agency sites;
- Official agency sites should not include confidential information and should conform to the Oklahoma Information Security Policy, Procedures and Guidelines;
- Official agency sites are subject to the Oklahoma Open Records Acts; and
- Agency information security representative and information technology and communications staffs should review the social networking, Web 2.0 or social media prior to launch;

8. Soft Launch/Testing

Perform usability testing both internally and with a small group of non-state agency employees. This testing will allow the agency to determine if the technology functions properly and meets the goals outlined in the business case.

9. Full Launch

After usability testing and any changes are made, let all interested parties know it is available for public use and promotion. State agencies should engage the State portal (OK.gov) to get the social networking, Web 2.0, or social media technology added to the State portal's list of social media assets. The agency marketing plan should also be employed to make the public, agency partners and other State governmental agencies aware of the launch.

10. Technical Maintenance

If a social networking, Web 2.0 or social media technologies are deployed on state agency servers, determine who is responsible for keeping the technology upgraded and patched for security vulnerabilities. In addition, determine what data needs to be backed up and on what schedule and who is responsible for the backups.

For externally-hosted social networking, Web 2.0 or social media technologies, identify when backups of the content are made, by whom and what is required to obtain copies of such backups.

Be sure to notify the designated agency disaster recovery coordinator. This information will be a part of the agency disaster recovery plan.

11. Monitor, Manage, Refine

All social networking, Web 2.0, or social media technologies should be reviewed annually to make incremental changes and ensure the social networking, Web 2.0, or social media technology is still viable for the current Internet community, provides a service as originally intended, and effectively communicates the agency message.

Appendix A – Sample Policy Covering Personal Devices, Universal Serial Bus (USB) Ports and All Removable Media

- USB ports are essential for most personal computers. They are universally allowed to support the connection of keyboards and mice. They can also be used for approved peripheral devices.
- The following are restricted USB devices: flash drives, memory sticks, audio/video devices (iPods, MP3 players or hybrids), cell phones or cell phone hybrids, micro drives or non-standard PDAs. Exceptions may be made to authorize the use of approved USB devices (specifically flash memory drives or external hard drives), if required to perform <Entity Name> activities, such as software installations and backup of existing files or systems.
- Only USB devices approved and provided by <Entity Name> can be used. If data resides on an unapproved USB device, it must be submitted to <Entity Name> so that it can safely be transferred to an approved device or a designated location on the network.
- All authorized USB devices used for data storage will include a data encryption algorithm and strong password support, both of which must always be used and cannot be removed.
- These guidelines apply to all <Entity Name> employees and anyone using <Entity Name> computer systems, including visitors, other state entity staff, contract staff and vendors.
- These guidelines must be followed to safeguard both personal and state information.
- No personal identity information, such as social security, tax identification, bank account, credit card, or drivers' license numbers shall be stored on these devices. Since state employee personal contact information, such as home phone numbers and addresses are considered sensitive information by state statute, storing this information is strongly discouraged. It will only be allowed for purposes of business continuity and/or disaster recovery planning and response.
- With regard to storing personal identity information, these rules and procedures apply to all forms of removable media, including CDs, DVDs, diskettes and all forms of tape storage used for any purpose other than backing up files for business continuity and disaster recovery.
- If any of these devices or media types are lost, stolen or accidentally destroyed, this action must be reported to your management and through the state incident reporting and management system.
- Violations of this policy, including abuse of administrator privileges, may be cause for criminal, civil, or disciplinary action up to and including termination.

Appendix B

Version History

The version numbering is as follows:

- The initial version is .1
- Once the deliverable has been accepted, it becomes version 1.00
- After the baseline (v1.00), all subsequent minor changes should increase the version number by 0. 1

Version Number	Change Request Number (*if applicable*)	Accepted Date	Author	Summary of Change
1.00		2/12/2010	Douglas Doe	
1.1		9/15/2011	Douglas Doe	Added information about terms of service agreements removed from policy and standards document by the GTARB
1.2		4/25/2013	Douglas Doe	Added section on Metrics/Analytics
1.3		11/25/2013	Douglas Doe	Changed references of OSF to OMES
1.4		09/30/2019	Jake Lowrey	Links updated.
1.5		10/18/2023	Jake Lowrey	Removed information about URL shortening services by Go.USA.gov which is not sunset; updated links.