OKLAHOMA
Office of Management
& Enterprise Services

# Social Networking & Social Media Guidelines

Revised February 2026

*Version 2.00 issued by OMES Outreach*

# Contents

# Section 1: Acceptable use

OMES regularly reviews social media and social networking technologies and their ability to empower state agencies and employees to more effectively communicate.

## 1.1 Separate personal and professional accounts

Employees should be mindful of blurring their personal and professional lives when administering social media and social networking sites.

### 1.1.1 Personal use

All state agency employees may have personal social networking and social media accounts. These accounts should remain personal in nature and be used to share personal opinions or nonwork-related information. Following this principle helps ensure a distinction between sharing personal and agency views.

State employees should not use their state agency email account or password in conjunction with a personal social networking or social media account.

During normal business hours, state agency employees may use personal social networking for limited family or personal communications so long as those communications do not interfere with their work and are in line with any state agency policies governing usage of these technologies.

The following guidance is for state employees who decide to have a personal social media or social networking account or comment on posts about official state business:

- State your name and, if relevant, role when discussing state agency or State of Oklahoma business.
- Use a disclaimer, such as "The postings on this site are my own and don't reflect or represent the opinions of the State of Oklahoma or the agency for which I work."

Executives and managers should take additional caution when posting to personal social media or social networking sites. By virtue of their position, they should consider whether published personal content may be misunderstood as expressing an official state agency position. Additionally, an executive should assume that staff will read what is written. For example, it is not appropriate to communicate a major policy change to employees using this medium, but it could be appropriate to post information about the rationale for the policy change or a request for feedback about the policy change.

### 1.1.2 Professional use

All official state agency-related communication through social media and social networking platforms should remain professional in nature and always be conducted in accordance with the agency's communications policy, practices and expectations. State employees should not

use official state agency social media or social networking sites for political purposes, to conduct private commercial transactions or to engage in private business activities. State employees should be mindful that inappropriate usage of official state agency social media and social networking sites can be grounds for disciplinary action. If social media and social networking sites are used for official state agency business, the entire state agency site, regardless of any personal views, is subject to best practices guidelines and standards.

Only individuals authorized by a state agency may publish content to an agency website or state agency social computing technologies. The State of Oklahoma and its agencies have established means to communicate “official” information. This communication comes from those designated to speak publicly on behalf of the state or an agency. Only these authorized persons, or their designee, may publish content to an official state agency website or social media or social networking site.

# Section 2: Development methodology

Prior to using or creating a social networking 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.

## 2.1 Create an agency policy

As established by 74 O.S. § 840-8.1, all state agencies should adopt a policy governing acceptable and unacceptable use of social networking 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 nonagency sites.
- Use of agency computers to access social networking 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.
- Personal devices, e.g., cellphones and laptops.

## 2.2 Define social networking and social media use

Before creating a social media account or using any social networking features on behalf of your agency, it’s important to clearly define your plan. Consider developing internal guidelines that answer the following questions:

- **Who:** Who is requesting this social media presence? Who will create and maintain the account or tool? Who will approve the content before it is posted?
- **What:** What exactly are you trying to create (e.g., Facebook page, blog, YouTube channel)? Define the scope of the project. What software or internet access is required? Do

the platform's terms of service/use violate any provisions of the Oklahoma Constitution or state statute? Are there any fees involved and is funding available for this project? What are your strategic goals for this social media presence? What performance metrics will you track to show progress toward those 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 or social networking technology being used.
- **How:** How often will content be posted or updated? What types of content will be posted (give examples of topics or categories of content)? How will content be approved? What does the approval process look like and how does it work? How will you measure the return on investment (ROI) for this effort?

These questions help ensure that social media is used responsibly and effectively in alignment with state standards. Having clear answers in place before launching a platform reduces legal and security risks while helping your agency stay on mission and maintain public trust.

## 2.3 Learn about security practices

Employees with access to social networking or social media technologies should 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 antivirus software is current.
  - Ensure antispyware 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 devices that access the internet.
  - In the event a personal social networking account needs to be used (such as business page admins), only assign admin privileges to employees who regularly require access to the agency account, and encourage additional security measures be taken by employees to further secure their personal account.
- **URL shortening**
  - URL shortening tools, such as tinyurl and Bit.ly, conceal the actual website link and can direct users to malicious websites. URL shortening tools should not be used without prior approval from the agency/division director.
- **Social engineering/phishing**

    - These sites are the No. 1 target for social engineering, phishing and malware attacks.
    - Identities are anonymous on the web; you may not be communicating with whom you think.
- **Passwords**
    - Your state employee username or password or network credentials should not be used on these sites.
    - Strong and unique passwords or passphrases should be used for each individual website.
- **Privacy**
    - Confidential information should not be posted online.
    - Professional and personal content on these sites should not be mixed.
    - No one should share personal information, travel plans or information about others without their consent.
    - Enable and utilize privacy features included with the social networking or social media sites.
- **Malware**
    - Custom-written video players may contain malware; think twice before you open them.
    - Do not visit unknown or untrusted 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.
    - Exercise caution when receiving private messages on a social networking or social media site; do not select any links or download any files from these messages.
- **Reporting**
    - Work with your agency IT staff to ensure your device is properly patched.
    - Always report cybersecurity incidents promptly to OMES Oklahoma Cyber Command via a ServiceNow ticket or following the process in the Oklahoma Information Security Policy, Procedures and Guidelines.

## 2.3 Outline content strategy

Before posting content to a social media or social networking platform, employees with access should clearly define its purpose and how it aligns with the agency's goals and communication strategy. Official agency postings to unofficial or third-party social media sites should:

- Require agency management approval before being published.
- Clearly identify the agency name.
- Not include confidential information.
- Adhere to accessibility standards.

## 2.4 Track performance metrics

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

- If you offer a service to your customers, you should measure how many of the engagements 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 (e.g., has the use of social media reduced reliance on print materials, paid ads or physical outreach efforts)?
- 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 helped the agency respond more favorably to requests and/or issues (e.g., how many public questions or concerns were resolved through social media interactions)?
- Did traffic to specific service portals (license renewals, applications, permits, etc.) increase after a campaign?
- Are event registrations or public meeting attendance tied to social media outreach?

**Tips for applying these metrics:**

- Pick a few key metrics that align with your agency's goals (e.g., service usage, event participation, public awareness).
- Track performance over time to look for patterns or improvements.
- Consider built-in analytics tools (like Facebook Insights, X Analytics, etc.) to collect and compare data. Additionally, social media management tools with cross-network analysis are available to state agencies through the SW1054 nonmandatory statewide contract.

## 2.5 Develop guidelines for official agency accounts

Agencies are encouraged to develop guidelines for governing their agency social networking or social media accounts. This guidance should include the following:

- Agency leadership should approve the 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 Act.
- Agency IT and communications staff should review the social networking or social media platform prior to launch.
- All agency content posted to public sites should adhere to accessibility standards.

## 2.6 Soft launch and test

Before publicly launching an official agency social media account or campaign, agencies should perform internal testing and controlled feedback loops to ensure the platform functions correctly, aligns with communication goals and reflects the agency's standards. Below are practical examples.

1. **Internal testing with a small group of agency staff:**
    - **Mock-post reviews:** Create sample posts and share them internally to test for tone, clarity and format consistency across platforms (e.g., how text truncates on Facebook versus X).
    - **Mobile versus desktop checks:** Review how profile images, banners and pinned content appear on mobile devices versus laptops and desktops.
    - **Accessibility check:** Test use of alternative text, color contrast and captioning images and videos to ensure accessibility compliance.
2. **Functionality and workflow testing:**
    - **Role-based access:** Confirm the correct user permissions are set for posting, scheduling, responding and analytics (especially on tools like Meta Business Suite, Sprout Social or Hootsuite).
    - **Content approval process:** Walk through your planned workflow to test how posts will be reviewed and approved before publishing.
3. **Feedback collection:**
    - **Survey reviewers:** Send a short survey (e.g., Microsoft Form) asking content reviewers about the clarity, usefulness and tone of the content.
    - **Document common questions:** Pay attention to repeated questions or confusion during the test phase. This can help shape your FAQ or social media guidelines for staff.

## 2.7 Full launch

Once usability is complete and any needed adjustments have been made, your agency is ready for a full launch of its social media presence. This is the stage when the account becomes public facing and actively promoted.

Steps to consider in the full launch:

- Notify internal stakeholders (e.g., agency leadership and communications team) that the platform is now live and ready for public engagement.
- Activate your marketing and communication plan to promote the launch across channels such as your agency website, email updates (e.g., through govDelivery), public meetings or events, and internal newsletters.
- Introduce the account publicly with a welcome post that explains the purpose of the platform, what kind of content users can expect and how the public can interact with your agency.

- Coordinate with partner agencies or programs to help amplify the launch and drive early engagement.
- Monitor early activity closely and respond to questions or comments to help build trust and set the tone for community engagement.

### 2.8 Technical maintenance

If a social networking or social media technology is 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 or social media technologies, identify when backups of the content are made, by whom and what is required to obtain copies of such backups.

You should notify the designated agency disaster recovery coordinator as this information is recommended to be part of the agency disaster recovery plan.

### 2.9 Monitor, manage, refine

All social media and networking technologies should be reviewed annually to assess their effectiveness and make any necessary updates. This review helps ensure a platform still serves its original purpose, remains relevant to current internet and user trends, and continues to communicate the agency's message clearly and effectively. Regular evaluations help agencies maintain a strong, consistent digital presence and adjust to changing communication needs over time.

## Section 3: General guidance

### 3.1 Adhere to the state standard for artificial intelligence

State agencies should conform to the Use of AI in Oklahoma State Government Standard when using AI systems to support social media work. Specifically, any AI-generated copy, images or recommendations must be carefully reviewed by a human for accuracy, style, tone and alignment with agency standards before posting. Avoid entering sensitive or confidential information (such as personally identifiable information (PII), financial, health, education or criminal justice data) into public AI tools when preparing content. Agencies must also ensure any AI-powered social media features (e.g., automated replies, content generation, analytics tools that use AI, etc.) have been reviewed and approved through the state chief information officer in accordance with the state AI standard.

### 3.2 Maintain accessibility

State agencies should treat accessibility as a core component of their social media strategy, not an afterthought. In accordance with the Accessibility of Information and Communication

Technology Standard, all official social content should be designed so Oklahomans with disabilities can perceive, understand and interact with it, in line with standards set forth by the American with Disabilities Act, Section 508 and the Web Content Accessibility Guidelines standards.

In practice, this means consistently:

- Adding meaningful alternative text for images.
- Providing accurate captions or transcripts for audio and video.
- Avoiding text-heavy graphics without an accessible text alternative.
- Using sufficient color contrast.
- Steering clear of flashing or visually overwhelming content.

Agencies should also use each platform's built-in accessibility features, spot-check posts for common barriers and remediate issues as they are identified so that social media remains an inclusive, effective communication channel for all audiences.

## 3.3 Respect copyright and fair use laws

Be sure to show respect for the laws governing copyright and fair use of copyrighted material owned by others, including those of the State of Oklahoma and state agency brands. To avoid any claims for infringement, do not quote more than short excerpts of someone else's work and always provide attribution. It is a better practice to link to or share others' work, when possible.

## 3.4 Exercise caution when sharing

Online content is not private. State employees should realize what they post will be around for a long time and could be shared by others. It is best practice to avoid identifying, discussing or posting multimedia of others – including clients, partners, vendors or co-workers – unless you receive written permission or give credit to the content owner.

## 3.5 Be respectful

State employees should respect their audience and co-workers. The state government community contains a broad employee base with a diverse set of customs, values and points of view. Don't be afraid to be yourself, but you should do so respectfully. You should not use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in the workplace. State employees should show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory – such as politics and religion.

It is best practice to ensure your communications are in good taste. Think about sensitivity when providing links to nonagency content. Redirecting to another site may imply an endorsement of its material.

## 3.6 Protect the brand

Only those authorized by the State of Oklahoma or an agency may use brand marks or logos in communications. Those who are not authorized should not include the agency logo, the Great Seal of the State of Oklahoma or program logos in personal blogs or postings. For more information and best practices for state branding, contact the Statewide Branding Office within the Oklahoma Department of Commerce.

## 3.7 Always speak the truth

Please be aware of making unsubstantiated claims. If you need to respond or make a comment on something specific, it is best to verify the facts and provide references or sources of information that are current.

## 3.8 Stay cool

One of the hallmarks of social media usage is creating dialogue. Unfortunately, people won't always agree on an issue. When confronted with a difference of opinion, it is best to express your points in a clear, logical way instead of picking fights. When making a correction, be mindful that you have done so. Sometimes, it's best to ignore a comment and not give it credibility by acknowledging it with a response.

- Government social media pages should comply with the First Amendment of the U.S. Constitution, meaning state agencies should not hide or delete public comments on agency social media and networking sites. The only exceptions typically include comments that contain true threats of violence, obscene language (as defined by the U.S. Supreme Court) or encouragement to violate state and federal laws.
- State agency social media admins should consult their legal department for specific guidance on hiding and deleting public comments from official agency social media pages.

## 3.9 Protect personal information

Astute criminals can piece together information you provide on different sites and then use it to impersonate you or someone you know – or even reset your passwords.

Similarly, posting real-time updates about your travels may confirm you aren't at home – letting someone target your house. Be careful when sharing information about yourself or others.

## 3.10 Don't be fooled

If you do post personal information on a social media or networking site, criminals can use it to send you emails that appear to come from a friend or other trusted source – even the site itself. This practice is called "phishing." Similarly, this ploy can also be used to infect your computer with a virus or keystroke logger.

### 3.11 Disable dangerous privileges

If a site allows others to embed code – such as HTML postings, links or file attachments – on your page or account, criminals can use them to install malicious software on your computer. If possible, disable the ability of others to post HTML comments on your site.

### 3.12 Heed security warning and pop-ups

There's a reason your security software provides warnings. You should not allow or select "yes" to digital action requests unless you know that they are safe.

## Section 4: User accounts

### 4.1 Account guidelines

In accordance with the Decentralized Security Representative (DSR) Standard, state agencies using social media or social networking technologies must submit all pertinent account information. This information includes but is not limited to employee name and username to manage the site, page, social media or social networking technology.

Pursuant to the Oklahoma Information Security Policy, Procedures and Guidelines, if an employee responsible for maintaining content of a site, page, social media or social networking technology leaves the state agency, their access to the technology shall be removed.

Changes to user account information must be provided to the agency's DSR using the previously detailed process.

### 4.2 Account names

#### 4.2.1 Overview

When creating government accounts on social media and networking platforms, it's important to select names that reflect the agency's identity, build trust with the public and align with the state's branding standards.

These guidelines are intended to:

- Help government organizations create consistent, recognizable names across platforms.
- Communicate authenticity when visual cues like a .gov domain are not available.
- Ensure account names clearly signal official government use.

The account name should:

- Reflect the agency's official name.
- Clearly convey the account is managed by a government entity.
- Leverage brand attributes such as trust, clarity and professionalism.

### 4.2.2 General guidelines

- Account names should remain consistent across platforms whenever possible.
- Be aware of platform-specific limitations (e.g., character limits or restrictions on special characters).
- It is recommended that all state agency account names include “ok” at the beginning to reflect official state representation.
- Example name variations due to constraints (Library of Congress):
  - **Website:** https://www.loc.gov
  - **Flickr:** library_of_congress
  - **YouTube:** libraryofcongress
  - **X (formerly known as Twitter):** librarycongress
- Passwords should conform to the standards detailed in the Oklahoma Information Security Policy, Procedures and Guidelines.
  - For security purposes, each social media account should have a unique password.
  - When platforms do not support separate login credentials (e.g., using a user’s login as a page admin), ensure admins use security features like multifactor authentication to prevent potential breaches in information.

### 4.2.3 State agencies

- Use recognizable acronyms (e.g., okdhs, okdot, okdps, okhca) only if they are widely known or if naming constraints force an abbreviation.
- Otherwise, use full or clear names that reflect the agency’s role (e.g., oklahomanursing, okcommerce, oklaforestry).
- Use a name that is as specific as possible, while clearly signaling the account represents an official state agency.

### 4.2.4 Programs

- Avoid acronyms unless widely understood by the public or required by character limits (e.g., OklahomaWIC).
- Use names that clearly represent the program’s purpose and official status (e.g., InsureOklahoma, OKTobaccoStops).

### 4.2.5 Individuals

- For official positions, role-based naming is recommended (e.g., okltgov, okgov, okattgen, oktreasurer, okcio).
- For elected officials with social media accounts used for official state business, a combination of title and name is recommended (e.g., RepFirstnameLastname, SenFirstnameLastname)
- Personal accounts (e.g., SteveJones) should only be used for nonstate- or noncampaign-related activity.

- Creating personal-name accounts helps protect your personal brand and prevent misleading information from being posted by someone else.

#### 4.2.6 Municipalities/counties

- Clearly identify as an Oklahoma city, town or county.
- Use naming that reflects both the place and its governmental nature.
- Examples: cityofokc, CityofShawneeOK, OklahomaCountyOK, BeaverCountyOK.

## 4.3 Account profile information

Create a complete agency-specific profile, indicating the agency and a description of the content. It is recommended that agencies do not use acronyms in profile data.

Account profiles should not include any personally identifiable information (PII). Limiting PII can help prevent identity theft and hackers from getting information that could be used in efforts to use social engineering to gain access to confidential information.

State agencies should prominently display contact information including at a minimum:

- Physical agency address.
- Agency main phone number.
- Agency general information email address, if available.
  - For security, agencies should avoid listing any email address that serves as a login or account name for any social media or networking technology.

## 4.4 Website linking

Linking websites helps the public and other state agencies find and verify agencies' official content. When used effectively, it drives traffic to reliable information and strengthens your agency's overall digital presence.

To ensure consistent and effective linking practices, agencies should follow these guidelines:

- Provide a clear link from the agency social media page back to the official agency website.
- If the social media account represents a specific subset of the agency – such as a program, campaign or newsroom – link directly to that relevant page within the agency site rather than the homepage.
- This not only confirms authenticity but also helps users quickly access more information or services related to the content they're engaging with.

# Appendix A: References

Links to resources referenced in this document, in order:

- ServiceNow ticket.
- Oklahoma Information Security Policy, Procedures and Guidelines.
- Use of AI in Oklahoma State Government Standard.
- Accessibility of Information and Communication Technology Standard.
- Decentralized Security Representative (DSR) Standard.

# Appendix B: Revision history

This guidance is subject to periodic review to ensure relevancy. The version numbering is as follows:

- The initial version is .01.
- Once the deliverable has been accepted, it becomes version 1.00.
- After the baseline (v1.00), all subsequent changes between publishing should increase the version number by 0.01.

| Version number | Accepted date | Author name | Summary of change |
|---|---|---|---|
| 1.00 | 2/12/2010 | Douglas Doe | |
| 1.01 | 9/30/2019 | Jake Lowrey | Minor style edits. |
| 1.02 | 9/25/2025 | Rowan Miller | Combined guidelines with SNSM methodology; added table of contents; content edits. |
| 1.03 | 12/05/2025 | Yahzmen Abraham | Minor phrasing edits. |
| 2.00 | 02/05/2026 | Christa Helfrey | Minor proofread, content additions and formatting edits. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |