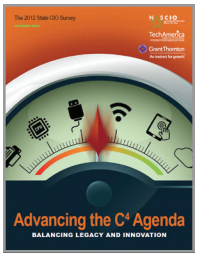
Examining State Social Media Policies: Closing the Gaps

It is estimated that more than 1 billion people around the world use social media. Not only has social media changed day-to-day operations but it has also substantially impacted the states in a variety of ways.

In 2010, NASCIO first broached the subject of social media in Friends, Followers and Feeds, where state governments were surveyed on social media adoption, use, and best practices. The survey examined adoption trends, current applications and expectations of social media technologies, the extent to which implementation is governed by formal policies or individual agency initiative, and perceptions of risk associated with social media tools. One of the most significant findings of the 2010 survey was that **social media adoption rates are broad across state governments; HOWEVER, two-thirds of survey respondents lacked enterprise policies addressing social media.**



In the 2012 NASCIO survey of state CIOs, Advancing the C4 Agenda: Balancing Legacy and Innovation, 100% of respondents reported that their states use social media in some manner. 83% use Facebook moderately or widely, while 81% use Twitter moderately or widely and 83% use YouTube moderately or widely. 80% of CIOs rated the future value of social media in state governments as "high" or "essential."

The 2012 survey also found that:

- No states are prohibiting the use of social media by their agencies;
- More than half the states already have policies and standards in place and another quarter are working on them;
- The majority of CIOs believe that social media are working to promote innovative state services.

NASCIO Contact:
Meredith Ward
Senior Policy Analyst
NASCIO

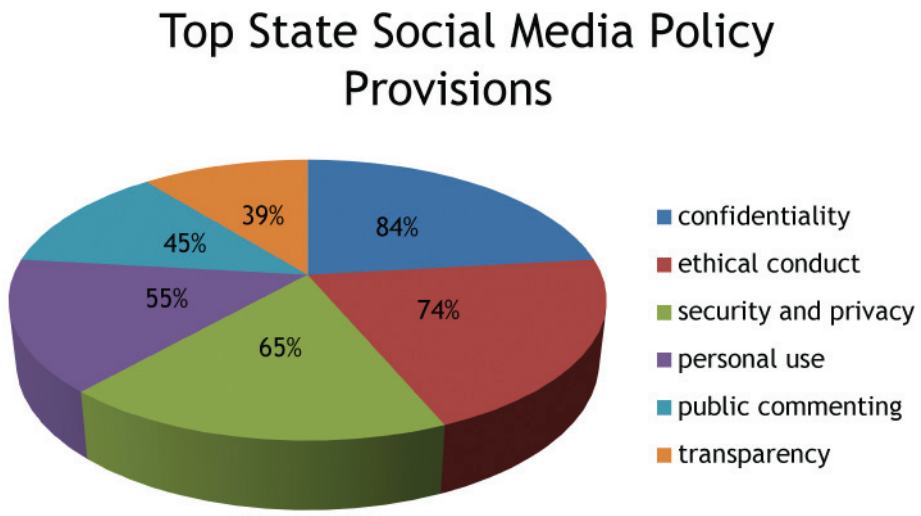
NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@AMRms.com
www.NASCIO.org

States have come a long way in the past few years, with the majority implementing social media policies or working towards one. However, we've only just begun. In early 2013, NASCIO's Legal Advisory Working Group took a look at 31 state social media policies, focusing specifically on guidance/policy given to state employees regarding their participation in social media. We will refer to these specific provisions as "social media participation policies," or "SMPPs." Some of the gaps found have the potential to open up states to some severe heartburn: including employee discontent, management concerns, public perception and liability.

The SMPPs surveyed addressed three aspects of state government employee participation in social media: (1) use of social media at work for purposes of fulfilling the employees' job responsibilities; (2) personal use of social media while at work and using the state employer's information technology and (3) personal use of social media outside of work hours in a manner related to his or her state employer.

Here is a summary of the most frequently occurring provisions in state SMPPs:



NASCIO source: content analysis of 31 state social media policies

Congress Shall Make No Law…

Less than half surveyed had policy language in place to govern public commenting and respecting commenter's First Amendment rights.

The visibility of negative posting on social media accounts is wide spread—slamming a business or government entity for real or perceived wrong doing. While imposing restrictions on obscene, threatening, discriminatory or harassing language is acceptable in conjunction with an appropriate, prominently posted comment policy, First Amendment principles likely do not permit agencies to delete negative or undesirable comments simply because they are critical. The precise contours of citizens' free speech rights in the context of state sponsored social media are currently unclear; this area of law is complex and evolving.

RECOMMENDATION:

In addition to social media participation policies, states should consider amending or adopting broader social media policies addressing issues such as amending privacy policies and terms of use to reflect use of social media.

Courts have not yet addressed a case where a public agency has been challenged for deleting comments made by citizens, corporations or other external commentators on agency blogs, wikis or interactive social media sites. This specific topic has been analyzed in some detail by University of Florida law professor Lyrissa Lidsky. As Professor Lidsky notes, "Social media have the potential to revolutionize discourse between American citizens and their governments. At present, however, the U.S. Supreme Court's public forum jurisprudence frustrates rather than fosters that potential."[1] A research paper available online is intended, in part, to help agencies navigate "the notoriously complex body of public forum doctrine to provide guidance for those who must develop or administer government-sponsored social media or adjudicate First Amendment questions concerning them."

RECOMMENDATION:

State CIOs should consult with their counsel about how free speech rights impact a state government's ability to withhold from publication, edit or delete citizens' speech on state government sponsored social media.

Post with Precaution

Another issue at hand is one that can spark much debate: the survey found that **just more than half had policy language in place governing personal use of social media by state employees**. When most employees in the United States take on gainful employment, we know that it is in our best interest to represent the employer in the best possible way in the office. It is also likely that most employers wish that employees positively represent the employer outside of normal business hours.

For example, as reported in the New York Times, Officer Trey Economidy of the Albuquerque Police Department was involved in a fatal on-duty shooting in early 2011. Much to Officer Economidy's regret, a local news station found his Facebook profile page which listed his occupation as "human waste disposal." Officer Economidy was placed on desk duty, and the Albuquerque Police Department now has a policy to govern officers' use of social networking sites.

An example from the National Labor Relations Board (NLRB) found that an ambulance company, American Medical Response of Connecticut (AMR), did violate the National Labor Relations Act (NLRA) when it fired an employee after she posted complaints over a work-related incident and about her supervisor from her home computer to Facebook. The NLRB found that the complaints were a protected concerted activity and the AMR policy limiting blogging and Internet posting were overly broad.[2]

RECOMMENDATION:

For the mutual protection of states and state employees, personal social media use must be clearly defined as personal and not representing the views of the state or agency.

[1] Public Forum 2.0, University of Florida Levin College of Law Research Paper No. 2011-08, Lyrissa Barnett Lidsky

[2] American Medical Response of Connecticut, Inc., NLRB Case No. 34-CA-12576 (2010)

Additional Findings:

The SMPPs also addressed

- Confidentiality: don't post private information (84%)
- Ethical conduct: represent the state well (74%)
- Security and Privacy: don't invite threats to the network and (again) don't post personal information (65%)
- Transparency: be authentic (39%)

As tools for state officials, we have included a legal and policy checklist and the Commonwealth of Massachusetts sample social media participation policy.

The bottom-line—the use of social media tools has exploded and such tools are being used throughout state governments across the country. The growing use of these tools, without comprehensive social media participation policies in place, puts states at legal risk of labor and employment law, First Amendment rights, and privacy and security. Whether a state is writing its first social media participation policy or updating an existing one, the SMPP samples posted on the NASCIO Community will be a resource for CIOs and their counsel.

RECOMMENDATION:

The NASCIO Legal Advisory Working Group encourages states to include in their policies essential language to protect states and employees.

SOCIAL MEDIA LEGAL ISSUES CHECKLIST

- ☐ 1. Authority to execute click through agreements with providers
- ☐ 2. Terms of service provisions
    - a. Binding contract
    - b. Objectionable provisions, "adhesion" contracts
        - i. indemnification
        - ii. limitations on liability
        - iii. endorsements or advertising
        - iv. jurisdiction and venue
        - v. choice of law
        - vi. copyright and intellectual property
        - vii. persistent cookies
        - viii. privacy policy
        - ix. data gathering practices
        - x. unilateral changes to terms without notice
    - c. Traps for the unwary
        - i. unpredictable legal consequences
        - ii. restrictions on permissible uses
        - iii. requirements, e.g. model releases for photo sharing sites, copyright ownership
- ☐ 3. Records
    - a. Records retention requirements
        - i. data hosted by third parties
        - ii. social media analytics
    - b. Public disclosure
    - c. Litigation holds/discovery
    - d. Note that employee posts of work info on private pages may subject personal social media accounts, home computers, or mobile devices to litigation holds, public records searches, etc.
- ☐ 4. First amendment and expression issues (particularly on blogs or in comments)
    - a. Policy to delineate limited public forum
    - b. Need to moderate or monitor
- ☐ 5. Intellectual property
    - a. rights to content published
    - b. responsibility to monitor user-generated content
    - c. limited protection
        - i. obscenity - Communications Decency Act
        - ii. infringing content - Digital Millennium Copyright Act
    - d. use of state seal/logos/agency name to market (branding)
- ☐ 6. Open Public Meetings Act compliance
- ☐ 7. Publicity rights (need for permission to publish photos, etc.)
- ☐ 8. Confidential information (inadvertent or intentional disclosure)
- ☐ 9. Ethics law
- ☐ 10. Rules of professional responsibility
- ☐ 11. Hijacking of agency or public official's identity, username infringement
- ☐ 12. Accessibility (nondiscrimination and ADA requirements)
- ☐ 13. Disclaimers/privacy policies

- ☐ 14. Privacy implications and commercial practices with respect to the stewardship of data
    - a. Children's Online Privacy Protection Act (COPPA)
- ☐ 15. Employment-related Issues
    - a. Pre-employment screening
    - b. Discrimination
    - c. Employee conduct
- ☐ 16. Technology advances more quickly than the law
- ☐ 17. Blurring of public and private roles (privacy)
- ☐ 18. Assessing legal risk

SOCIAL MEDIA POLICY ISSUES CHECKLIST

- ☐ 1. Agency process to assess business needs and approve use
    - a. Who, what, where, when, why, and how; risks and benefits
        - i. Clear direction on authority to establish accounts/execute click through agreements
        - ii. Clear direction on who will read and assess terms of service
- ☐ 2. Identify and consider all potential agency concerns – e.g., management, public information, information technology, information technology security, risk management, legal, public records and records retention, contract administration, human resources, program needs
- ☐ 3. Scope of policy
    - a. Authorized business use
        - i. Agency operations
        - ii. Investigative and law enforcement purposes
        - iii. HR use
            1. Pre-employment screening
            2. Post-employment
                - a. employee behavior issues
                - b. monitoring of use
                - c. internal investigations
    - b. Professional networking
        - i. Potential collective bargaining issues
    - c. Personal use (de minimis)
        - i. Potential collective bargaining issues
- ☐ 4. Definitions – social networking, types of social media and associated terms
- ☐ 5. Interactions with the public
- ☐ 6. Records retention
- ☐ 7. Relation to existing policies, e.g. internet privacy, acceptable use of internet, ethics
- ☐ 8. Employee education
    - a. Terms of use restrictions
    - b. Legal issues
    - c. Policy
    - d. Social networking best practices, etiquette, and "norms"

COMMONWEALTH OF MASSACHUSETTS SAMPLE SOCIAL MEDIA PARTICIPATION POLICY

Social Media Participation Policy

1. Introduction

This document formalizes the policy for employees that are managers, non-union employees and contractors ("users") within the [INSERT AGENCY NAME] on the use of social media sites. ***This policy shall also extend to bargaining unit members, except that Section 3 (Required Work-Related Use of Social Media) shall apply to such members only if they have voluntarily agreed in writing with their employer to the use of social media as a job responsibility.***

"Social media sites" refers to websites that facilitate user participation, networking, and collaboration through the submission of user generated content. A "social media identity" is a specific user identity or account that has been registered on a third party social media site (such as the Whitehouse account on Twitter™ or an employee's personal account on Facebook™). Social media in general includes tools such as: blogs, wikis, microblogging sites, such as Twitter™; social networking sites, such as Facebook and LinkedIn™; video sharing sites, such as YouTube™; and bookmarking sites such as Del.icio.us™.

This document addresses three distinct uses of social media, including:

a. **Required Work Related Use of Social Media:** Use of social media that is sanctioned as part of employee's job function (e.g. when an employee tweets on behalf of the Executive Director of the Agency on the Executive Director's Twitter account). This use is addressed in Section 3 of this policy.

b. **Personal Use of Social Media at Work:** An employee's personal use of social media while at work (e.g. logging onto Facebook and providing personal updates to a Facebook page, which is outside of the employee's official job function, while at work, during work hours). This use is addressed in Section 4 of this policy.

c. **Personal Use of Social Media Outside of Work:** An employee's use of social media in his or her personal capacity outside of work time. This use is addressed in Section 5 of this policy.

2. User Responsibilities

It is the responsibility of any person subject to this policy that uses a social media to read, understand, and follow this policy. In addition, users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of social media identities. Any person with questions regarding the application or meaning of this policy should seek clarification from appropriate management. Failure to observe this policy may subject individuals to disciplinary action, including termination of employment.

3. Required Work-Related Use of Social Media

The [Agency name] is pleased to announce the launch of a new social media channels to communicate with customers. A social media identity is a specific user identity that has been registered on a third party social media site and is associated with the Agency, an official at the Agency, or a designated employee. Government social media sites or identities typically provide forums for commentary or news on topics related to the government agency that hosts the social media site or has secured the social media identity. A typical social media site (whether hosted by the Agency or a third party) combines text, images, and links to other websites including blogs, wikis, and other media related to the topic and enables readers to leave comments in an interactive format.

The purposes of [Agency name]'s social media identities and sites include [sample goals …

- Engaging in conversation with the citizens of the Commonwealth of Massachusetts
- Furthering the goal of transparency within government
- Providing the agency with meaningful feedback from our customers
- Goal 4…]

This document outlines the policy for [Agency name] employees' conduct while contributing to or moderating this Agency's social media sites or providing comments or updates to the Agency's social media identities.
In addition to the topics addressed here, social media content must be in compliance with the [Agency name]'s relevant policies, including its harassment and discrimination policies, confidentiality policies, ethics rules, code of conduct, and other policies.

Social media Guidelines

a. **Follow the Acceptable Use Policy.** Know and follow [Agency's Name]'s Acceptable Use Policy (the "AUP") and any additional acceptable use policies for use of Commonwealth information technology resources adopted by your agency. Your agency's social media site or identity is an "information technology resource" under the AUP.

b. **You are Personally Responsible for What you Publish.** You are personally responsible for the content you publish on your agency social media site. Be mindful that what you publish will be public for a long time.

c. **Considerations When Speaking on Behalf of your Agency.** Identify yourself—name and, when relevant, role at your agency—when you discuss agency or agency-related matters on your agency social media website or in connection with the Agency's social media identity. Write in the first person. It is important to make clear when you are speaking for yourself, and when you are speaking on behalf of the agency. Only speak on behalf of the agency when your commentary is based on the law governing your agency, or on your agency's explicit written stan-

dards, policies, and practices, or you have received prior permission from your supervisor to address a particular topic in a particular way. However, there are occasions when agency employees will be asked on a social media site (such as a blog or wiki), as they are by the public in other situations, to explain how the laws to which the agency is subject, or the regulations and policies that it has issued, or its historic practices, will apply to a particular situation. There is often no black letter law, regulation, or policy, or historic practice, that addresses with 100% certainty an issue raised by the public. In their daily work with the public, state employees appropriately, on occasion, answer such questions by interpreting known precedents. When they do so, state employees often say something like "I don't know what the official agency position would be in that situation, but in my opinion, …". When faced with a similar question on a social media site, make clear, as you would if speaking in person or over the phone, that you are offering your opinion on a matter, not the agency's official position.

d. **Understand Users' First Amendment Rights.** Although the [Agency name] can moderate the social media sites that accept comments from the public (such as blogs and wikis) to restrict speech that is obscene, threatening, discriminatory, harassing, or off topic, we cannot use the moderation function to restrict speech with which the [Agency name] merely disagrees (i.e. subject matter restrictions). Users have some First Amendment rights in posting content to public social media sites hosted by state agencies. Moderators must respect those rights by posting all comments other than those excluded for specific legitimate reasons, such as those identified in the [Agency name] Terms of Comment [link].

e. **Do Not Comment on Social Media Sites about Agency Business Outside the Agency's Social Media Sites or Identities.** Do not publish content to any website outside of your agency's website that has to do with that agency or agency-related matters.

f. **Respect Copyright Law.** [Agency name] social media participants must abide by laws governing copyright and fair use of copyrighted material owned by others. Never reprint whole articles or publications without first receiving written permission from the publication owner. Never quote more than a short excerpt of someone else's work and, if possible, provide a link to the original.

g. **Protect Confidential Information.** Don't provide your agency's confidential information. Never post legally protected personal information that you have obtained from your agency (e.g., information that is not public record under the Public Records Law, Mass. Gen. L. ch. 66, sec. 10 or whose dissemination is restricted under the Commonwealth's Privacy Act, Mass. Gen. L. ch. 66A, Executive Order 504, or under other Federal or State privacy laws or regulations). Ask permission to publish or report on conversations that occur within your agency. Never post information about policies or plans that have not been finalized by your agency, unless you have received explicit permission from your supervisor to post draft policies or plans on the agency social media for public comment.

h. **Consider Your Content.** As informal as social media sites are meant to be, if they're on a government domain or a government identity, they're official government communications. Social media sites will be sought out by mainstream media – so a great deal of thought needs to go into how you will use the social media in a way that benefits both the [Agency name] and the public.

i. **Don't Feed the Rumor Mill.** You should merely say, "no comment" to rumors. Do not deny or affirm them—or suggest either denial or affirmation in subtle ways.

j. **Handling Negative Comments.** Because the purpose of many social media sites particularly agency blogs and wikis, is to get feedback from the public you should expect that some of the feedback you receive will be negative (and you may need to develop a thick skin!). Some effective ways to respond to negative comments include:

    i. Providing accurate information in the spirit of being helpful

    ii. Respectfully disagreeing

    iii. Acknowledging that it is possible to hold different points of view

k. **Provide Links.** When you make a reference to a law, regulation, policy, or other website, where possible provide a link or at a minimum, the cite.

l. **Respect Your Audience and Your Coworkers.** Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in your agency's workplace. Remember that the Commonwealth's residents reflect a diverse set of customs, values and points of view. Don't be afraid to be yourself, but do so respectfully. This includes not only the obvious (no ethnic slurs, personal insults, obscenity, threats of violence, etc.) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory—such as party politics and religion. Do not use your agency's social media presence to communicate among fellow Commonwealth employees. Do not air your differences with your fellow Commonwealth employees on your agency's social media's presence. Show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory—such as race, ethnic origin, and religion.

m. **Be Transparent, Admit to your Mistakes, and Differ Respectfully.** Don't pick fights, be the first to correct your own mistakes, and don't alter previous posts without indicating that you have done so. When you see misrepresentations made about your agency by media or by other users, you may use the agency's social media site or identity to point that out. However, you must do so with respect, and stick to the facts.

n. **Use the Social Media Site or Identity Only to Contribute to your Agency's Mission.** When you contribute to your agency's social media site or identity provide worthwhile information and perspective that contributes to your agency's mission of serving the public. What you publish will reflect on your agency and the Administration. Social media sites and identities should be used in a way that contributes to the agency's mission by:

    i. Helping you and your co-workers perform their jobs better;

    ii. Informing citizens about government services and how to access them;

    iii. Making the operations of your agency transparent and accessible to the public;

    iv. Creating a forum for the receipt of candid comments from residents about how government can be improved; and

    v. Encouraging civic engagement.

o. **Respond to Your Own Mistakes.** If you make an error, own up to it and correct it quickly.

    The [Agency name] policy is that once something is posted, it should stay posted. Only spelling errors or grammar fixes should be made without making the change evident to users. If you choose to modify an earlier post, make it clear that you have done so—do not remove or delete the incorrect content; provide the correct information and apologize for the error. Ways to accomplish this include:

    i. Strike through the error and correct

    ii. Create a new post with the correct information, and link to it from the post you need to correct or clarify.

    Either method is acceptable. The goal is that for the social media identity or site to achieve transparency, we cannot change content that has already been published without making the changes clearly evident to users.

p. **Use Your Best Judgment.** If you're about to publish something that makes you even the slightest bit uncomfortable, review the suggestions above and think about why that is. If you're still unsure, discuss it with your manager.

q. **Don't Forget Your Day Job.** Make sure that your online activities, even if they are sanctioned or required by your agency, do not interfere with other parts of your job. Employee social media users are responsible for keeping their managers informed about any impediments that arise which could disrupt the agreed on publishing schedule.

r. **Handling Media Inquiries.** The [Agency name] social media identity or site may lead to increased inquiries from the media. If you are contacted directly by a reporter, you should refer media questions to the [Agency name] [INSERT NAME OF REFERRAL].

4. Personal Use of Social Media at Work

a. **Follow the Acceptable Use Policy.** Know and follow [Agency's Name]'s Acceptable Use Policy (the "AUP") and any additional acceptable use policies for use of Commonwealth information technology resources adopted by your agency. Access to third party websites using Commonwealth technology is an "information technology resource" under the AUP.

b. **Employees' personal use should not be attributable to the agency or to the employee's job function at agency.** An employee's use and comments made at a social media site are subject to First Amendment protections. However, any personal use made of social media sites while at work (for example during break periods), must be conducted in such a manner that a reader would not think that the employee is speaking for or on behalf of his or her agency employer.

c. **Must be in conformance with relevant portions of workplace policies and all relevant laws and regulations.** Employees' use of such sites must be in compliance with the [Agency name]'s relevant policies, including its harassment and discrimination policies, confidentiality policies, ethics rules, code of conduct, and other policies, as well as with state Ethics Law, Federal Copyright law, and other applicable laws and regulations.

d. **Must not be excessive.** Excessive use of social media during work hours may result in discipline or termination.

5. Personal Use of Social Media outside of Work

a. **Employees' personal use should not be attributable to the agency or employee's job function at agency.** An employee's use and comments made at social media sites are subject to First Amendment protections. However, any personal use made of social media sites outside of work assignments or responsibilities, where such personal use is related to subject matter pertinent to the employee's agency, must be conducted in such a manner that a reader would not think that the employee is speaking for or on behalf of his or her agency employer.

b. **Must be in conformance with relevant portions of workplace policies.** Employees use of such sites must be in compliance with the applicable portions of the [Agency name]'s relevant policies, including its harassment and discrimination policies, confidentiality policies, ethics rules, code of conduct, workplace violence, and other policies. Some of these policies, for example the Agency's sexual harassment policy and the ethics rules, could apply to employee actions performed outside of normal working hours at third party sites.