NATIONAL LEAGUE of CITIES | RISK INFORMATION SHARING CONSORTIUM

Building Local Government Social Media Policies

Social media is a new world of opportunity for local governments to communicate with citizens and receive feedback. Its risks are similar in nature to those of other types of communication, but with a different twist because material circulates so widely and there are many potential contributors. One recommended tool for addressing these risks is to adopt a social media policy. But what should be in that policy? It is not an easy question to answer.

Many local government social media policies are posted online, but this is an area where one size definitely does not fit all. Social media policies do not stand in isolation. They usually incorporate related policies by reference, and policies that address other issues are often amended to include social media specific provisions. Thus, social media policies are often a web of interrelated policies. Each government must take an individual approach to ensure that all these diverse parts come together to meet its unique needs.

Pools have a strong interest in their members' management of social media risks. They can help their members develop a social media policy by providing suggestions about what a social media policy should do. To assist RISC member pools in this outreach, NLC-RISC has prepared these recommendations about the building blocks for a social media policy. This resource can be used by the pool as a starting point for preparing its own guidelines or can be distributed to pool members under its name.

Control and structure of the government's official social media

Failure to control when and how social media sites are being created and used on behalf of the government sets the stage for losses. The first task for a social media policy is to establish the control structure for the government's official social media program. Three major issues are who has the authority to:

- Establish and terminate official social media accounts.
- Develop and implement the government's social media strategy.
- Develop and enforce a social media policy.

Some governments centralize control over their official social media presence. Centralized programs restrict who can establish an account and require prior review by an identified authority for all posts or comments on behalf of the government. Centralized control has an advantage from the risk control

perspective. It establishes authority and accountability and reduces the chances of a deviation from policy that results in liability.

Other governments decentralize control over their official social media presence to accommodate their operations' different goals and objectives. For example, emergency management may want to tweet alerts and recreation may want to post its activities on a Facebook page. A government might give those operations significant control over their social media presence so they can more nimbly accomplish their goals.

Not all decentralization is the same. The most decentralized approach is a policy that gives some guidelines about acceptable and prohibited use but otherwise allows agencies the freedom to establish social media accounts and pursue their own strategies. A more conservative approach would be a policy that decentralizes day-to-day control subject to general guidelines, but requires prior approval to establish a social media site and designates someone to monitor all the government's social media resources and order necessary changes. For risk control purposes, the more conservative approach offers the advantage of consistent oversight to ensure compliance with policy, combined with a degree of freedom to allow operations to take full advantage of the real-time nature of social media.

Small governments that plan relatively limited use of social media – for example a single Facebook page for the city – will probably use centralized control. Larger governments are likely to have a more decentralized social media program. Both will benefit from a social media policy that outlines the government's official position on social media, identifies who is authorized to participate in the government's official social media sites, and guides them on its implementation. Most of the approaches outlined below are consistent with either a centralized or decentralized approach.

Public records

One of the most difficult issues in local government use of social media is how to comply with the state's public records laws. Some social media posts are akin to casual conversation, but others pertain to official government business. Even comments posted by members of the public may qualify as public records, including those that have been removed as violating the public comment policy. How to draw the line between social media content that does and does not qualify as public records, identify the content that must be retained, and develop an archiving system are all issues of concern to governments using social media.

Many social media policies simply require compliance with the local government's existing public records policy. Three specific social media policy

provisions that an government can consider to facilitate compliance with public records laws are:

- Post all original content to the government's website and use the social media site as a secondary outlet.
- Link back to the official government website for additional information.
- Require employees who post public records to a social media site to ensure that the original document is retained in a manner that complies public record policy.

Guidelines for employee use of the government's official social media

Guidelines for employee use of the government's official social media are a critical part of a social media policy. Even if only one employee posts and responds to comments, that employee must know what is expected and the government must have some way of holding the employee accountable.

The guidelines for use derive from what can go wrong in a social media environment. Some of the major concerns are the following:

- Bad information that misleads the public and causes harm
- Violation of intellectual property rights
- Disclosure of private or confidential information
- Harassment
- Defamation

Any of these can lead to claims and lawsuits. The goal of guidelines is to prevent adverse outcomes.

Guidelines for employee use of the government's official social media encourage some conduct and prohibit other conduct. Some examples of useful positive requirements include:

- Be honest and transparent.
- Post only within one's area of expertise.
- Post only useful information.
- Keep it professional - avoid confrontation.
- Be accurate.
- Correct errors, and if modifying an earlier post, identify the change.
- Be responsive to citizen concerns.
- Adopt a user name that follows a standard format and clearly identifies the user as a city employee.

Employees should be prohibited from posting:

- Information about actual or potential claims and litigation involving the government.
- The intellectual property of others, without written permission.

- Photographs of employees or members of the public, without written permission.
- Defamatory material.
- Any personal, sensitive or confidential information about anyone.
- Obscene, pornographic or other offensive/illegal materials or links.
- Racist, sexist, and other disparaging language about a group of people.
- Sexual comments about, or directed to, anyone.
- Political campaign materials or comments.
- Threatening or harassing comments.
- Other information that is not public in nature.

The policy should also address the sanctions that will be imposed for breach of the policy. Be consistent with, or simply incorporate by reference, the employee discipline policy.

Many of these issues may already be addressed in other policies that can be incorporated by reference or used as a resource. In particular, any code of conduct or ethics should be incorporated by reference. Be consistent with or incorporate by reference website, information technology, communication, media relations, public information and privacy and confidentiality policies should also be considered.

Guidelines for employee use of other social media

Many employees already have purely personal social media accounts they use to interact with friends and family. They also may participate in "professional" social media that are related to their work or profession, but are not their employer's official site and usually are not a part of their job. An example of professional social media is GovLoop, a social networking site for government workers. Another example is LinkedIn. An employee also might establish a page on what is traditionally a personal social media site, such as a Facebook, for purposes of networking with professional colleagues.

Active participants in professional social networks can gain useful information that will help them do their jobs better, but they may also be more likely to discuss the details of their job on those sites. Their identification with a specific employer means that their posts can easily reflect upon the employer.

Personal and professional social media sites pose risks to the government even if employees access them when they are off-duty and using their own personal devices. Major risks include:

- Disclosure of private or confidential information
- Posting photographs of fellow employees or citizens without their permission

- Harassment
- Retaliation
- Defamation

Looking first at purely personal social media, the entity has little control over employees' actions in their free time using their own personal social media accounts and their own devices. Despite this lack of control, the exposures for the government are very real. Employees sometimes use their personal social media to discuss their jobs and post work-related photographs or information that expose the government to liability or compromise its confidential information. Many interact with co-workers, even with their supervisors/subordinates, and real or perceived slights, harassment, retaliation or discrimination can follow them into the workplace.

Many employees also use personal social media during work hours, either through the government's or the employee's personal technology, such as a smart phone. Personal use of social media through government technology has all the same risks identified above, as well as:

- Reduced work performance
- Downloading to government servers and distributing the same inappropriate content that may be accessed through the Internet.
- Inappropriate use of government property for political, commercial or criminal activity.

A government can prohibit social media at work and adopt blocking and/or monitoring programs for its own technology equipment. These techniques likely will not eliminate the use of personal social media at work, as many employees now have access to social media through their smart phones. However, they will help keep inappropriate content off government servers.

Monitoring employee use of social media and disciplining employees for violating a no-use policy have their own risks. Employees may claim that monitoring invades their privacy and constitutes an unreasonable search. Whether or not the government routinely monitors employees, notify employees in writing that they have no expectation of privacy in their use of government technology. Include the notice in the government's technology policy. If the government needs to access the employee's computer, the notice provides a defense. Also avoid taking job action against an employee based solely on monitoring results. Other factors, such as performance, should be considered.

Professional media sites pose many of the same risks as purely personal sites. They are also more likely to be accessed during work time using the government's technology, often with the government's explicit approval or encouragement. Because professional social media specifically relates to

professional interests, the employee is more likely to be identified with the government and discuss its business than on a purely personal social media site. Disclosing confidential information, casting the government it in an unfavorable light, and misrepresenting the government's position are all risks.

To address these risks, consider including in the social media policy:

- A requirement that employees include in any post related to the government or their job on a personal or professional site a disclaimer that the posting reflects their own opinion, and not that of the government.
- By reference, policies that relate to conduct and ethics, privacy and confidentiality, harassment, retaliation and other relevant conduct.
- If monitoring employee use of social media at work, written notice of the nature and scope of monitoring.
- Notice that employees have no reasonable expectation of privacy when using government technology.
- If access of personal social media through government technology is permitted, notice that employee use of personal social media at work must be brief, not interfere with performance of the employee's duties or with the workplace, and not involve commercial, political or other prohibited activities.

Guidelines for elected official use of social media

Elected officials' use of the government's official social media or their personal or professional social media can raise many of the same risks just discussed with regard to employees. Elected officials who use the city's official social media should be subject to the same requirements as employees. (For open meetings purposes, discussed below, they may not want to use the official social media.) Many local governments have codes of ethics for elected officials, sometimes combined with the code for employees, which can be adopted by reference into the social media policy.

A risk that is different for elected officials is possible violation of the state's open meetings laws through the use of social media. A quorum of lawmakers holding a discussion about public business through social media may constitute a meeting that is subject to the open meetings law. This could happen through the official government social media, and some governments consequently prohibit elected officials from participating in their official social media. Equally problematic is elected officials' use of their own social media to communicate in their official capacity with members of the public. Informal communication with constituents is generally acceptable, but discussion of public business is risky, especially if it involves other elected officials. The dynamic nature of social media and the sheer volume of posts may make it difficult to track who is involved in the discussion and detect when the open meetings line has been crossed.

Another potential risk associated with elected official use of social media is use of government resources for political purposes. Elected officials are increasingly using social media for campaign purposes. Elected officials who use the same social media for communicating with constituents as they do to campaign risk violating the law against using government resources for political purposes.

To address these risks, consider including in the social media policy:

- Recognition that elected official use of social media to discuss public business may violate the open meetings law.
- A prohibition against elected officials using any social media (personal, professional or the government's official social media) to discuss public business.
- A requirement that a social media site used by an elected official to communicate with constituents include a link back to the city's official website for detailed information.
- A requirement that elected officials who use social media for campaigning establish separate social media for that purpose and not access that social media through government technology.

Public comment on the government's official social media

Some governments use their social media as a one-way communication tool to flow information to members of the public. Those governments disable comment features on their social media. Others view social media as an opportunity to receive information and feedback from the public and enhance operations. For example, members of the public might be encouraged to post a report of potholes, rather than calling.

The benefits of public comments have accompanying risks. A member of the public may post content that is inappropriate by being off-topic, defamatory, harassing, obscene or pornographic, criminal, or commercial. Or a citizen may just post an opinion that is critical about some aspect of the local government.

The risks of permitting public comments include:

- Failure to act on information reported by a member of the public resulting in harm to someone. If a member of the public posts a comment about a dangerous condition on public property, the government has notice. If it does not take action to address the dangerous condition and someone is injured or killed, a lawsuit may result.
- Although it would seem obvious that posts to social media are not private, members of the public who post may be disturbed if their comments are disclosed as public records under the state's open records law.

Other significant risks associated with public comment arise from what the government does (or does not do) to manage it. These include:

- Failing to monitor and remove inappropriate comment.
- Government employees responding inappropriately (in a harassing manner) to public comments.
- Violating the free speech rights of members of the public by removing comment based on the viewpoint or opinion expressed.

To address these risks, consider including in the social media policy:

- A public comment policy for posting on the social media site that does the following:
    - Identifies viewpoint neutral criteria that will be used to determine when a comment or link posted by a member of the public will be removed, which can include comments that are off-topic, obscene or pornographic, defamatory, harassing, commercial, criminal, political, or that violate the intellectual property rights of others.
    - Reserves the right to remove posts that violate the policy.
    - Gives notice that the comments are monitored only during business hours, and thus information conveyed after hours will not be received until the next business day.
    - Gives notice that comments are subject to disclosure as public records.
- Procedures and responsibility for monitoring of public comments and removal of inappropriate comments in accordance with the public comment policy.
- Procedures and responsibility for monitoring, responding to, and taking timely action to act upon information conveyed via public comments.

Conclusion

There are risks to undertaking any new activity, but social media is a powerful tool for local governments looking for new and cost-effective ways to engage their citizens. Just be sure to adopt social media with due consideration and planning. This means having clear objectives, knowing the target audience, selecting the right social media for the task, and taking the time to develop the right policy. Social media evolves quickly, so it is a good practice for the social media policy to remain platform neutral, and to review and revise it frequently to meet the changing environment.