North Carolina Department of Cultural Resources

Best Practices for Local Government Social Media Usage in North Carolina

April 2010

1. PURPOSE

The role of technology in the 21st century workplace is constantly expanding and now includes social media communication tools that facilitate interactive information sharing, interoperability, and collaboration. Commonly used social media Web sites, such as Facebook©, Twitter©, MySpace™, YouTube©, Flickr®, Blogger, and LinkedIn®, have large, loyal user bases and are, thus, increasingly useful outreach and communication tools for government entities from the federal to the local level.

Moreover, a social networking presence has become a hallmark of a vibrant and transparent communications strategy. Social networking improves interactivity between a local government and the public, and it reaches populations that do not consume traditional media as frequently as others do. Therefore, local governments should consider using social networking Web sites to enhance their communications strategies. In doing so, however, local governments should take care to choose the types of social networks that make the most sense for their type of information and that give emphasis to tools that provide more information across multiple outlets to the broadest audience.

All government communication tools should be used in ways that maximize transparency, maintain the security of the network, and are appropriately professional. Social media is no exception. Therefore, the application of social media in local government must be done thoughtfully and in a manner that minimizes risk. In addition, social media users should be aware that these types of communications are considered public records and, consequently, must be kept for a certain period of time in compliance with the public records law. These guidelines are intended to ensure that local governments' social networking sites[1] are secure and appropriately used and managed by outlining "best practices" for the use of social media. Thus, the suggestions provided in this document are designed to protect government employees and ensure consistency across entities when incorporating social media into their mission.

2 RECOMMENDATIONS

2.1 IMPLEMENTATION

Every government should have a clear communications strategy and should take the time to determine how social media fits into this strategy. The following questions should be considered when determining whether use of social media is appropriate:

[1] This document is not meant to address one particular form of social media, rather social media in general, as technology will inevitably change and new tools will emerge.

- Who is the media meant to reach? Is this my target audience?
- What is the organization attempting to communicate? Can it be effectively communicated using this media?
- Who is responsible for managing the organization's account? Will this person represent the organization appropriately? Has he or she been properly trained in the use of social media?
- What are the organization's responsibilities regarding collection and records retention including preservation of social media content? What does the records retention schedule require for these records?

When a local government decides to use a form of social media that is deemed beneficial to its mission it should first set up boundaries for using the service. It is recommended that an account administrator is assigned to spearhead the use of social media within the workplace. Account administrators and other potential users are encouraged to complete online training for social media in tutorial form on the North Carolina Department of Cultural Resources Web site, www.records.ncdcr.gov.

Account administrators are encouraged to create internal policies that keep track of social media domain names in use and the associated user identifications and passwords currently active. Should the employee who administers the account be removed as administrator or no longer be employed by the organization, all passwords and account information should be immediately changed to maintain organization control.

2.2 ACCEPTABLE USE

All use of social networking sites by local governments should be consistent with applicable state, federal, and local laws, regulations, and policies including all information technology security policies. This includes any applicable records retention and disposition schedules or policies, procedures, standards, or guidelines promulgated by the Department of Cultural Resources. All usage should be governed by these policies as well as the recommendations in this document and future internal policies.

Following are specific recommendations for acceptable use of social media sites:

Separate Personal and Professional Accounts:
Employees should be mindful of blurring their personal and professional lives when administering social media sites.

Personal Use:
Employees are allowed to have personal social networking sites. These sites must remain personal in nature and be used to share personal opinions or non-

work related information. This helps ensure a distinction between sharing personal and organizational views. In addition, employees should never use their government e-mail account or password in conjunction with a personal social networking site.

Professional Use:
All government-related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the organization's communications policy, practices, and expectations. Employees must not use social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Employees should be mindful that inappropriate usage of social media can be grounds for disciplinary action. If an account is used for business, the entire account, regardless of any personal views, is subject to these best practices guidelines and the records retention schedule, including the collection and preservation provisions.

Be Clear As To Identity:
When creating social media accounts that require individual identification, government employees should use their actual name, not pseudonyms. However, using actual names can come with some risks. Any employee using his or her name as part of a local government's application of social media should be mindful of the following:

- Do not assume privacy. Only post information that you are comfortable disclosing.
- Use different passwords for different accounts (both social media and existing work accounts). Using the same password for all accounts increases the vulnerability of the accounts being compromised.

Terms of Service:
Employees should be aware of the Terms of Service (TOS) of the particular form of media. Each form of social media has its own unique TOS that regulate how users interact using that particular form of media. Any employee using a form of social media on behalf of a local government agency should consult the most current TOS in order to avoid violations. If the TOS contradict organization policy then a decision should be made about whether use of such media is appropriate.

Content of Posts and Comments:
Employees using social media to communicate on behalf of a local government should be mindful that any statements made are on behalf of the organization; therefore, employees should use discretion before posting or commenting. Once these comments or posts are made they can be seen by anyone and may not be able to be "taken back." Consequently, communication should include no form of profanity, obscenity, or copyright violations. Likewise, confidential or non-public

information should not be shared. Employees should always consider whether it is appropriate to post an opinion, commit oneself or one's organization to a course of action, or discuss areas outside of one's expertise. If there is any question or hesitation regarding the content of a potential comment or post, it is better not to post. There should be great care given to screening any social media communication made on behalf of the organization as improper posting and use of social media tools can result in disciplinary action.

Posts and Comments Are Public Records:
Like e-mail, communication via government-related social networking Web sites is a public record. This means that both the posts of the employee administrator and any feedback by other employees or non-employees, including citizens, will become part of the public record. Because others might not be aware of the public records law, local governments should include the following statement (or some version of it) somewhere on the social networking Web site:

Representatives of [insert specific local government] communicate via this Web site. Consequently any communication via this site (whether by a government employee or the general public) may be subject to monitoring and disclosure to third parties.

2.3 SECURITY

From a security standpoint, local governments should be mindful of how to best prevent fraud or unauthorized access to either the social media site or the government network. In almost every case where an attacker accesses a system without authorization, they do so with the intent to cause harm. The harm intended may be mild or more serious.

Thus, security is an ever-present concern that must be addressed. If participating in social media, local governments should:

- Ensure that employees are made aware of which information to share, with whom they can share it, and what not to share.
- Provide security awareness and training to educate users about the risks of information disclosure when using social media, and make them aware of various attack mechanisms.
- Ensure that employees are aware of Privacy Act requirements and restrictions. Educate users about social networking usage policies and privacy controls to help them better control their own privacy in any profile they use for work-related activities and more effectively protect against inadvertent disclosure of sensitive government information.

2.4 RECORDS MANAGEMENT AND PRESERVATON

Communication through local government-related social media is considered a public record under G.S. 132 and will be managed as such.

- All comments or posts made to local government account walls or pages are public, not private.
- Account administrators who receive messages through the private message service offered by some social media sites should encourage users to contact them at a public e-mail address maintained by their organization. For private messages that account administrators do receive, they should be treated as constituent e-mails and therefore, as public records. Account administrators or other authorized staff members should reply using their government e-mail account.
- Local governments should set all privacy settings to public.

Local governments must assume responsibility for public records and comply with the retention period set forth in their approved retention and disposition schedule. Local governments must assign their own schedule of collection and disposal for social networking Web sites according to the administrative value of the record and permanently retain records with historical value. Refer to Web Site Guidelines policies on North Carolina Government Records Web site (http://www.records.ncdcr.gov/erecords/default.htm).

3. CONCLUSION

Social media is an effective and efficient way for local governments to communicate with and participate in the larger community. It will continue to shape and support the way they communicate and collaborate with constituents as they strive to provide an accountable and transparent government. As local governments use social media they need to strike a balance between providing access to information and securing their government's core network. This document is meant to help local governments understand these risks and outline some best practices for social media usage.