North Carolina Office of the Governor

North Carolina Office of Information Technology Services

North Carolina Department of Cultural Resources

Best Practices for State Agency Social Media Usage in North Carolina

Version 2.0

March 2012

TABLE OF CONTENTS

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 important outreach and communication tools for government entities from the federal to the local level.

Moreover, a social networking presence has become a hallmark of vibrant and transparent communications. Social networking improves interactivity between a state agency and the public, and it reaches populations that do not consume traditional media as frequently as others do. Therefore, state agencies and departments of all types are encouraged to enhance their communications strategies by using social networking Web sites. In doing so, however, state agencies 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 agency 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 within state agencies must be done thoughtfully and in a manner that will minimize 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 state agencies' social networking sites are secure and appropriately used and managed by outlining "best practices" for the use of social media in North Carolina state government. Thus, the suggestions provided in these guidelines are designed to protect state employees and ensure consistency across agencies when incorporating social media into their mission.

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. Also, the guidelines in this document do not apply to the innovative tools related to workflow efficiencies such as "wikis" or other intra-office tools used for document sharing.

2. GUIDELINES

2.1 IMPLEMENTATION

Every agency should have a clear communications strategy and should take the time to determine how social media fits into this strategy. Agency Public Information Officers (PIOs) should spearhead this activity and, in doing so, should consider the following questions when determining whether use of social media is appropriate:

- Who is the media meant to reach? Is this my target audience?

- What is the agency attempting to communicate? Can it be effectively communicated using this media?

- Who is responsible for managing the agency's account? Will this person represent the agency appropriately? Have they been properly trained in the use of social media?

- What are the agency's responsibilities regarding collection and records retention including preservation of social media content? What does the records retention schedule require for these records? Will the Department of Cultural Resources be able to archive this material for us or will we need to archive it ourselves? If we have to archive it ourselves, how will we do this?

When an agency decides to use a form of social media that is deemed beneficial to its mission it should first establish employee boundaries for using the service. It is important for agency supervisors to communicate expectations of appropriate usage for the media within the workplace.

Social media sites, as much as possible, should be established for the agency rather than in the name of an individual employee. There should be an authorization process for employees wishing to create an account for the benefit of the agency, with the agency PIO as the authority to oversee and confirm decisions. In this role, the PIO will evaluate all requests for usage, verify staff being authorized to use social media tools, and confirm completion of online training for social media.

PIOs will also be responsible for maintaining a list of all social networking application domain names in use, the names of all employee administrators of these accounts, as well as, the associated user identifications and passwords currently active within their respective agencies. Should the employee who administers the account be removed as administrator or no longer be employed by the agency, the PIO should immediately change all passwords and account information to maintain agency control.

The Department of Cultural Resources is able to collect most social networking content using an automated Web harvesting tool. PIOs should consult with DCR to determine the best method to archive the content and to make sure those archiving the content are aware of the account. If an agency decides to take down their social media sites, please contact the Department of Cultural Resources prior to the deletion to ensure that the content is captured. Any agency-related social networking usage implemented prior to the release of this document should be reviewed by the agency PIO to make sure it is brought into compliance with these guidelines.

In summary, under this suggested workflow PIOs will:

- Oversee and confirm decisions regarding the appropriateness of using social media sites including authorization of sites

- Evaluate requests for usage

- Verify staff being authorized to use social media tools

- Maintain a list of social media domains, active account logins and passwords

- Change passwords if employee is removed as administrator in order to maintain agency control

- Consult with DCR to ensure social media material is archived including providing DCR staff a list of all social media urls and account contact information[1]

2.2 ACCEPTABLE USE

All use of social networking sites by state agencies should be consistent with applicable state, federal, and local laws, regulations, and policies including all information technology security policies. This includes the agency and statewide acceptable use policies and 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 guidelines in this document.[2]

Separate Personal and Professional Accounts:

Employees should be mindful to not blur 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 agency views. In addition, employees should never use their state e-mail account or password in conjunction with a personal social networking site. As with other technologies,

---

[1] Please visit www.webarchives.ncdcr.gov to submit a url for inclusion in DCR harvest of websites.

[2] Please visit www.records.ncdcr.gov and https://www.scio.nc.gov/mission/itPoliciesStandards.aspx

employees may utilize social media sites for personal use during business hours. If they have not done so already, state agencies should consider crafting a policy regarding employees' personal use of social media sites during normal business hours.

Professional Use:

All agency-related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the agency'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 and all communications made via it, including those reflecting personal views, is subject to these best practices guidelines, including the collection and preservation provisions.

Be Clear As To Identity:

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

- Do not assume privacy. Only post information that appropriately represents your agency.

- 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.

- Whenever possible, do not administer professional accounts using personal account information. Doing so may cause personal information, such as "likes," friends, photos, or personal posts to be linked to a professional account. Government pages should not reflect personal views or favorites. Employees should be mindful that social media sites frequently change their settings. As a result, employees should constantly monitor their professional pages to ensure inappropriate content does not appear on them.

Terms of Service:

Employees should be aware of the Terms of Service (TOS) of each social media site. Each has its own unique TOS that regulates how users interact using that particular form of media. Any employee using a form of social media on behalf of a state agency

should consult the most current TOS in order to avoid violations. If the TOS contradict agency policy then the PIO should be made aware and 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 state agency should be mindful that any statements made are on behalf of state government; 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 deleted. 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 agency 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. A great deal of consideration should be put into each agency posting since improper posting and use of social media tools can result in disciplinary action.

Posts and Comments Are Public Records:

Like e-mail, communication via agency-related social networking Web sites is a public record. This means that both the posts of the account 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, agencies should include the following statement (or some version of it) somewhere on the social networking Web site:

Representatives of North Carolina state government communicate via this Web site. Consequently any communication via this site (whether by a state employee or the general public) may be subject to monitoring and disclosure to third parties.

2.3 SECURITY

From a security standpoint, agencies should be mindful of how to best prevent fraud or unauthorized access to either the social media site or the state 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, such as:
- making unofficial posts, tweets or messages—possibly of an embarrassing nature—that will be seen by the public as official messages,

- using the compromised site to spread malware, or

- encouraging users to either click links or download unwanted applications that the attacker has added to the site.

In some cases, the intended harm may be more serious. For instance, attackers could access the network and obtain information that could be used to compromise or disable the state system, State employees' information, or citizens' information.

Since security is an ever-present concern, it should always be considered when working in any web-enabled system.

Methods Used to Breach IT Security

It is important to note that security related to social media is fundamentally a behavioral issue, not a technology issue. In general, employees unwittingly providing information to third parties pose a risk to the core state network. Consequently, employees should know the major threats they may face and how to avoid falling prey. Prevalent social media security risks include third-party spear phishing, social engineering, spoofing, and web applet attacks.

Due to the relative vulnerability of social media sites to these security exploits, it is important to be cautious when using such sites. In order to prevent potential harm, users of social networking sites should minimize the amount of information an attacker is likely to gain from a successful attack. For example, individual user IDs and passwords should not be duplicated across multiple sites. In this way, if one site is compromised, the attacker cannot also gain access to other sites for which the user is authorized.

In particular, because of the importance of proper operation of the State network and the sensitivity of information stored on State systems within the network, a State employee must never use a current NCID password as a password on any other site.

If agencies participate in social networking, agencies should:

- 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 as described in this document,

- ensure 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 agency information, and

- educate users about specific social media threats before they are granted access to social media websites.

2.4 RECORDS MANAGEMENT AND PRESERVATON

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

- All comments or posts made to state agency accounts are public, not private.

- In the spirit of transparency in state government, account administrators who receive messages through the private message service offered by the social media site should encourage users to contact them at a public e-mail address maintained by their agency. For private messages that account administrators do receive, they should be treated as constituent e-mails and therefore, as public records. Account administrators or another authorized staff member should reply using their state e-mail account.
- Some social media services may provide integrated messaging services that streamline e-mail, private messaging, instant messaging or "chat" services, etc. into one package. All agency-related records created within the use of an integrated service package are "public," regardless of form. Therefore, account administrators should apply the behavior described above with regards to these communications as well.

- Agencies should set all privacy settings to public.

Agencies must assume responsibility for public records and adhere to the schedule of collection for social networking Web sites set by the North Carolina State Archives. The Department of Cultural Resources is able to collect most social networking content using an automatic Web harvesting tool. If an agency wants the Department of Cultural Resources to collect their social networking content, that agency must provide the Department of Cultural Resources with a current list of all active account domain names and not delete any information or communication threads before archival harvesting has been completed for a particular scheduled harvest. Some social media services may enable users to choose privacy features that will inhibit harvesting. Agencies should not activate such features (i.e., a secure socket layer [SSL]) since this will prevent compliance with the Web harvesting process and could cause the account administrator to be in violation of the public records law.

Agencies may rightfully decline to participate in the automated harvesting performed by the Department of Cultural Resources. If an agency does decline or if the Department of Cultural Resources notifies a PIO that they are unable to collect the content using the automated harvesting capability, then the agency must manually archive the public

content on their own. Refer to Web Site Guidelines policies on North Carolina Government Records Web site (http://www.records.ncdcr.gov/erecords/default.htm). Agencies manually archiving their social media content should not rely on social media service providers to store their content, as this removes control of these public records from the agency itself. Thus, allowing a third party to make decisions about retention of public records and impeding the agency's ability to live up to their responsibility to identify and enable retrieval of this content.

Instead, agencies should maintain a local copy of the content from their social media sites. Keeping a copy of this content on a local, networked, state-owned server ensures compliance with the public records law and allows the agency to provide the required level of public access to these materials.

In addition, agencies manually archiving their social media content are not relieved of the records management obligations related to it once they stop using social media tools. Instead, these agencies should determine which of these records are required to be retained and for what time period in accordance with the policies set by the Department of Cultural Resources and the applicable Records Retention and Disposition Schedules.

If an agency is closed or consolidated, the PIO or their designate should contact the Department of Cultural Resources to ensure that the social media sites are being collected. You can access all archived content at www.webarchives.ncdcr.gov.

3. CONCLUSION

Social media is an effective and efficient way for agencies to communicate with and participate in the larger community. It will continue to shape and support the way agencies communicate and collaborate with constituents as they strive to provide an accountable and transparent government. As agencies use social media they need to strike a balance between providing access to information and securing the state's core network. To find that balance, each agency needs to assess its risk. This document is meant to help agencies and their users understand these risks and outline some best practices for social media usage. Every agency should adopt these tools and provide their employees support and guidance to use them productively and intelligently.

Appendix – Definitions

Copyrighted material – includes materials that may be protected by Copyright Law (for example, a cartoon, article, or excerpt from a book). In other words, if the information or material is copyrighted, it may not be publicly circulated without prior authorization from the copyright holder.

Cross-Site Scripting (XSS) - a security vulnerability which allows attackers to insert code into a target user's web page.

E-mail message – a single electronic mail message sent directly to another user.

Identity Spoofing - involves one person, system, or website successfully masquerading as another by falsifying identity-related information and thereby being treated as a trusted user or system by another user or program.

Post – comment made to a user's social networking page or site. For example, Facebook users can post to another user's "wall."

Record – data or information in a fixed form that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference. A record has fixed content, structure, and context. (Society of American Archivists Glossary)

Retention and disposition schedule – a document that identifies and describes an organization's records, usually at the series level, provides instructions for the disposition of records throughout their life cycle. (SAA Glossary)

Social engineering – an attack that involves gathering and using personal information about a target in a deceitful manner in order to convince the target to provide the attacker permissions to obtain or access restricted information.

Social networking – the use of a variety of Web sites that allow users to share content, interact, and develop communities around similar interests.

Spear phishing – an attack targeting a specific user or group of users, attempting to deceive the user(s) into performing a routine action, such as opening a document or clicking a link, which the phisher has booby-trapped to launch an attack.

Terms of Service (TOS) – rules by which one must agree to abide in order to use a service. It is generally assumed such terms are legally binding.

URL Spoofing - an attack in which a legitimate web page is reproduced on a server under the control of the attacker and then a target is directed to this site, thinking that they are on the legitimate site.

Web Applets - code routines, scripts or utilities that interact dynamically with web pages to provide additional functionality to the user.