County of Caldwell
P.O. Box 2200
905 West Avenue
Lenoir, North Carolina 28645
Telephone 828-757-1300
Fax 828-757-1295
www.caldwellcountync.org

CALDWELL COUNTY POLICY FOR SOCIAL MEDIA USAGE

1. PURPOSE

The role of technology in today's workplace is continually expanding and includes social media communication tools that facilitate interactive information sharing, interoperability and collaboration. Commonly used social media Websites, such as Facebook ©, Twitter©, Snapchat©, YouTube©, and LinkedIn®, have large loyal user bases and are increasingly important outreach communications tools for local government entities.
Moreover, a social networking presence has become a hallmark of a vibrant and transparent communications strategy. Social networking improves interactivity between Caldwell County and the public, and it reaches populations that do not use traditional media as frequently as others. Therefore, Caldwell County departments and agencies are encouraged to enhance their communications strategies by using social networking Websites. In doing so; however, county departments and agencies must 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 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 and; therefore, the application of social media within county departments and 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 public records and must be maintained for periods of time as determined by the public records law. This policy provides guidelines intended to ensure that social networking sites, maintained by county departments and agencies, are secure and appropriately used and managed. These guidelines are designed to protect county employees and ensure consistency for departments and agencies incorporating social media into their mission.

2. GUIDELINES

2.1 IMPLEMENTATION

Every department and agency must have a clear communications strategy and take the time to determine if and how social media fits into this strategy. Those departments and agencies choosing to utilize social networking sites should designate an employee(s) within the department or agency to lead this activity. The following questions should be considered when determining whether the use of social media is appropriate:

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

- What is the department attempting to communicate? Can it be effectively communicated using this media?
- Does the department want to elicit feedback from citizens? What media is best suited to allow for the type of interaction desired?
- Who is responsible for managing the department's account? Will this person represent the department appropriately? Have they been properly trained in the use of social media?
- What are the department's responsibilities regarding collection and records retention including preservation of social media content? What does the records retention schedule require for these records? How will we collect and store the media content?

When a department 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 department heads and supervisors to communicate expectations for appropriate usage for the media within the workplace.

There should be an authorization process for employees wishing to create an account for the benefit of the department with the department head, or designee, having the authority to oversee and confirm decisions. The department head, or designee, must evaluate all requests for usage, verify staff being authorized to use social media tools and confirm completion of online training for social media. The department head, or designee, is also 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 departments. Should the employee who administers the account be removed as administrator, or no longer be employed by the department, the department head, or designee, should immediately change all passwords and account information to maintain department control. Departments must send the name of the person designated to oversee department sites along with site name and type to the county Public Information Officer who is responsible for maintaining a master list.

The Information Technology Department will provide assistance to help determine the best method to archive the content. Any department social networking usage implemented prior to the approval and implementation of this policy must be reviewed by the department head, or designee, to ensure and bring into compliance with these guidelines.

In summary, department heads, or designees, will:

- Oversee and confirm decisions regarding 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 department control.
- Ensure social media material is archived including providing a list of all social media URLs and contact information.

2.2 ACCEPTABLE USE

All use of social networking sites by county departments must be consistent with all applicable laws, regulations and policies including the Electronic Communications Policy and all information technology security policies. This includes the department and county acceptable use policies and any applicable Records Retention and Disposition Schedules or policies, procedures, standards or guidelines promulgated by the North Carolina Department of Cultural Resources. All usage must be in compliance with the before mentioned policies as well as the guidelines in this document.

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

Personal Use:
The county supports every employee having personal social networking sites; however, those sites must remain personal in nature and be used to share personal opinions or non-work related information. This helps ensure a clear distinction between sharing personal and county views. In addition, **employees should never use their county e-mail account or password in conjunction with a personal social networking site** and employees should never refer or link to their personal site(s) from their county site. Employees should remain mindful of their responsibilities under the county's E-Mail Policy and Code of Conduct Policy when posting on the internet.

Professional Use:
All department related communication through social media outlets should remain professional in nature. Employees must not use social networking sites for political purposes, to conduct private commercial transactions or to engage in private business activities. Sites containing anything racially or sexually discriminating or of a political or religious nature are prohibited. Employees must remain mindful that inappropriate usage of social media are grounds for disciplinary action up to and including termination of employment. Thus, if an account is used for business, the entire account, regardless of any personal views, is subject to these guidelines, including the collection and preservation provisions.

Be Clear As To Identity:
When creating social media accounts that require individual identification, county 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 county department'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 password for all accounts increases the vulnerability of the accounts being compromised.

Term 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 county department should consult the most current TOS in order to avoid violations. If the TOS

contradicts county policy, then the Public Information Officer should be made aware and a decision made as to whether the use of such media is appropriate.

Content of Posts and Comments:

Employees using social media to communicate on behalf of a county department should be mindful that any statements made are on behalf of county 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 withdrawn. Consequently, communications 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 department 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 communication made on behalf of the department using this social media as improper posting and use of social media tools can result in disciplinary action.

Posts and Comments Are Public Record:

Like e-mail, communication via department related social networking Websites 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, can become part of the public record. Information on social media sites has little or no historical value; therefore, content will not be retained in most cases. Because others might not be aware of the public records law, departments should include the following statement somewhere on the social networking Website:

> *Representatives of Caldwell County government communicate via this Website. Consequently, any communication via this site (whether by a county employee or the general public) may be subject to monitoring and disclosure to third parties and is considered public.*

Caldwell County Comment Policy:

These social media sites provide the opportunity to present matters of public interest in Caldwell County, including its many residents, businesses and visitors. We encourage you to submit your questions, comments and concerns, but please note this is a moderated online discussion site and not a public forum.

It should be further noted that service requests should not be submitted through comments on any Caldwell County social media site. Service requests must be submitted through established procedures.

Once posted, Caldwell County reserves the right to delete submissions that contain:

- Vulgar language.
- Personal attacks of any kind.
- Offensive comments that target or disparage any ethnic, racial or religious group.

Further, Caldwell County also reserves the right to delete comments that are:

- Spam or include links to other sites.
- Clearly off topic.
- Advocate illegal activity.
- Promote particular services, products or political organizations.
- Infringe on copyrights or trademarks.
- Use personally identifiable medical information.

Please note that the comments expressed on these sites do not reflect the opinions or positions of the Caldwell County government or its officers and employees. If you have any questions concerning the operation of this online moderated discussion site, please contact the Caldwell County Public Information Officer.

2.3 SECURITY

To safeguard employees and departments it is imperative to be mindful of how to prevent fraud or unauthorized access to either the social media site or the county 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 on 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 county system, county employees or citizens. In this scenario, attackers could acquire information such as:

- Confidential information about county employees or citizens.
- Sensitive security information.
- Data about public safety plans, or,
- Defenses currently in place against attacks on public facilities.

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 county 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.

As a result of 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 county network and the sensitivity of information stored on county systems within the network, a county employee must never use a current county password as a password on any other site.

If departments participate in social networking, they should:

1. Ensure that employees are made aware of which information to share, with whom they can share with and what not to share.
2. Provide security awareness training regarding the risks of information disclosure when using social media and make them aware of various attack mechanisms as described in this document.

3. Educate employees about specific social media threats before they are granted access to social media websites.

2.4 RECORDS MANAGEMENT AND PRESERVATON

Communication through department related social media is considered a public record under North Carolina General Statutes, Chapter 132 and will be managed as such.

- All comments or posts made to county department account walls or pages are public.
- In the spirit of transparency in county government, account administrators who receive messages through the private message service offered by the social media site should direct the user to contact them at a public e-mail address maintained by their department. Alternatively, account administrators could reply to the inquiry using their county e-mail account. Departments should set all privacy settings to moderated. Comments expressing an opposing view point must be allowed.

Departments must assume responsibility for public records and adhere to the schedule of collection for social networking websites set by the North Carolina State Archives.

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 departments use social media they need to strike a balance between providing access to information and securing the county's core network. To find that balance, each department needs to assess its risks. This document is meant to help departments and their users understand these risks and outline some best practices for social media usage.

Adopted this 3rd day of February, 2020

Randy T. Church, Chairman

Thomas Welch II, Clerk to the Board

This policy supersedes all previously published policies regarding this subject.