City & County Attorney

LEGAL GUIDE TO SOCIAL MEDIA

ArchiveSocial

INTRODUCTION

Tweets, comments, and shares have become the new currency of communication throughout the world. These abbreviated signals are the new lingua franca in an era of instant, two-way communication that connects the physical world digitally with social media. This connectivity is such a powerful bridge that over 74 percent of people in the United States now spend more time on social media than on any other online activity—and it's growing. Over time, social media has evolved from connecting people-to-people to connecting people-to-business and now, it's connecting people-to-government.

The early government adopters of social media primarily used it as a tool to broadcast information online, but even that has changed. Social media now serves as a primary interface between government and citizens for virtually every service government provides to the public. In today's connected world, social media is used to solicit crime tips, report potholes, request clarification in regards to community programs, coordinate during emergencies, and conduct many other tasks that were once relegated to phone calls, letters, and in person trips to City Hall. Like any new medium that increases transparency and communication, social media also introduces new risks and liabilities that city and county attorneys must address.

In a survey conducted by the Center for Digital Government, only half of the selected government agencies utilizing social media had the necessary policies in place to ensure legal protection.

This guide provides an overview of the key issues and actionable recommendations for mitigating risks through the use of social media policy and technology. This guide was created in collaboration with the Center for Digital Government, ArchiveSocial, and Julie Tappendorf—a leading attorney for social media issues in the public sector.

Chapter 1:
LEGAL ISSUES TO CONSIDER WITH SOCIAL MEDIA

Social media has introduced many new issues that impact everything from public records law to free speech. Each of these issues must be carefully balanced when developing internal and external policies for employees and citizens. This chapter is designed to provide an overview of the key legal issues affecting social media usage by the government. In Chapter 2, we provide guidance for crafting social media policies that address the issues highlighted in this chapter.

EMPLOYEE USAGE OF SOCIAL MEDIA

Personal vs Professional Social Media Profiles

In today's environment, the individuals responsible for representing your agency on social media likely also manage a presence on social media for their own personal lives. Ideally, these individuals are able to manage your agency's business through specialized social media profiles created for the agency, and refrain from conducting public business on their personal Facebook and Twitter profiles. Unfortunately, it can be easy to violate this separation in practice—particularly if employees are not well-informed regarding policies and procedures. In particular, it is often challenging for public officials to separate day-to-day community issues from their personal identities. Mayors in cities across America, ranging Florida to New Mexico, have faced legal challenges due to their use of social media to conduct public business in a manner non-compliant with governmental requirements.

Discipline of Current Employees

Outside of failing to separate public business from their personal profiles, evidence of misconduct related to work performance that is gathered from social networking sites may be an appropriate basis for action against current employees. The misconduct must impact, or have a nexus to, the reputation of the employer or the employer's ability to deliver services to the citizens. For example, if a police officer posts obscene pictures on his or her Facebook page, or photos of obvious illegal conduct, this will likely serve as an appropriate basis for disciplinary action.

Can an employer terminate or discipline a worker for complaining about his or her boss or company on Facebook? Will social media policies protect an employer? In one case, the National Labor Relations Board (NLRB)[1] ruled that a nonprofit employer unlawfully discharged five employees who had posted comments on Facebook relating to allegations of poor job performance that had been previously expressed by one of their coworkers. The workers were found to be engaged in "protected concerted activity" because they were discussing terms and conditions of employment with fellow co-workers on Facebook. In another case[2], however, the NLRB ruled that a reporter's Twitter postings did not involve protected concerted activity. Encouraged by his employer, a reporter opened a Twitter account. He began posting news stories which were sometimes critical of the newspaper. The newspaper terminated the reporter based on his refusal to refrain from critical comments that could damage the goodwill of the newspaper. The NLRB found that the employee's conduct was not protected and concerted because it (1) did not relate to conditions of employment and (2) did not seek to involve other employees on issues related to employment.

In addition, public employers have additional protections in the employee speech realm. A public employer cannot be disciplined or terminated for speaking on "matters of public concern." This means if a public employee is posting on Facebook about alleged government corruption or is supporting a political candidate, he or she has certain protections that must be taken into consideration before an employer takes any disciplinary action against the employee.

What does this mean for employers?

First, employers must be cautious in disciplining or terminating employees for critical posts on social media sites. An employer should ask itself whether the posts are "protected and concerted activity" or "matters of public concern" (both protected speech) or do the posts merely constitute "gripes" about an employer that are not protected? Second, an employer should review its social media policy to make sure it is not overbroad in prohibiting protected activities. Finally, an employer should be careful not to enforce social media policies in an arbitrary or discriminatory manner.

Employer Requests for Social Media Passwords

It has become common practice for employers to review the publicly available Facebook, Twitter, and other social networking sites of job applicants as part of the vetting in the hiring process. However, because many social media users have privacy settings that block the general public (or non-friends or followers) from viewing their complete profile, some employers have asked job candidates to either turn over their passwords or log on to their social media accounts during the interview.

Until a few years ago, there was no federal or state law expressly prohibiting this practice, although a few states have proposed or enacted legislation. Over the past few years, many states have adopted legislation prohibiting employers from seeking job applicant's social media passwords. For example, Illinois P.A. 97-0875 allows candidates to file lawsuits if they are asked for access to sites like Facebook. Employers can still ask for usernames to view public information and monitor employee usage of social media on employer devices.

What's the bottom line?

With respect to viewing a current employee's social media sites, unless there is an actual need to review an existing employee's social media profile, it may be difficult to find a connection between social media use and the employee's right to hold their job.

FIRST AMENDMENT CONCERNS

One of the most beneficial aspects of social media is that it creates an ongoing conversation between the public and the government. However, this interactive aspect can quickly become a potential minefield of legal issues for governments, particularly where comments and speech are involved. As this area of law is yet undeveloped, the public sector should proceed with caution so as to avoid running afoul of the First Amendment.

The Question of Public Forums

Whether a social media site is considered a "public forum" is an open question, raising concerns as to whether a government can remove allegedly objectionable Facebook comments without implicating First Amendment protections. While a social media site is not likely to be deemed a "traditional" public forum, it may be considered a limited or designated forum. That means a government can restrict or limit speech, but those restrictions or limitations are not limitless. Some commentators suggest that government social media sites should be treated the same as websites, which are treated as "government speech," meaning the government has complete control over the message. This premise is illustrated by the seminal case[3] on the issue, in which the courts ruled that a school district need not allow opposing viewpoints on a website entirely in its control. Social media sites, however, are controlled by private third parties (Facebook, Twitter, etc.) and there is far less government control over the message and content posted by others. The court specifically noted in Page v. Lexington that it may have ruled differently if the government's website had transformed into a type of "chat room" or "bulletin board" in which private viewers could express opinions or post information.

Furthermore, several recent legal situations have directly raised First Amendment concerns in regards to social media postings removed by government agencies.

A gun dealer in San Diego County made public comments on a Sheriff's Department Facebook page, until officials administering the page banned him and deleted his statements. The case[4] settled out of court when the Sherriff's Department became concerned about entering a legal minefield with hundreds of thousands of dollars in attorney's fees.

In a 2012 lawsuit, the Hawaii Defense Foundation challenge the City and County of Hawaii with free speech violations when a comment was deleted from the police department's page[5]. Honolulu agreed to settle the case by covering $31,610 in attorneys' fees for the plaintiff. The settlement was an unfortunate setback for the industry given that there are a variety of situations—such as when dealing with obscene content or hateful speech—in which comment moderation serves an important purpose.

PUBLIC RECORDS LAW

It is commonly understood that government emails are official communications, subject to all applicable public records laws. It is critical to recognize an agency's communications across social media sites must be treated in the same way. Federal agencies in the United States must retain records of social media in accordance with the Freedom of Information Act (FOIA). State and local governments must comply with similar state-specific records laws, which typically have a name such as Freedom of Information Act, Public Records Act, or Open Records Act. Because these existing laws were written in a manner that applies

to communications "regardless of physical form", it is not necessary to amend the existing records laws to identify social media as a form of communication requiring retention. Rather, several states have simply issued guidance clarifying the need to retain social media in accordance with public records requirements. Ultimately, it is the content of the communication that matters, not the format in which it is shared. In other words, a crime tip received via email is no more or less a record than a crime tip received via a Facebook private message, and each must be retained accordingly.

Many states have issued specific guidance clarifying that social media content is in-fact public record.

Oregon
"Like other forms of communication, social media posts are public records. That means they require you to retain them."

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

Texas
"Social media sites may contain communications sent to or received by state employees, and such communications are therefore public records subject to State Records Retention requirements. These retention requirements apply regardless of the form of the record (digital text, photos, audio, or video, for example)."

Attorneys must be aware that agencies across the country are receiving public information requests for social media content, and the volume of such requests is increasingly rapidly. Here are a two such examples:

- In 2014, the Santa Barbara Police Department in California was requested by the National Rifle Association to produce all social media communications regarding a gun buyback event. For more information, read the Government Technology Case Study.
- In 2015, the Vineland Police Department in New Jersey received monthly public information requests from a citizen concerned about comments being hidden from the department's Facebook page. For more information, read the Government Technology Case Study.

Outside of requests that specifically identify social media content, agencies are finding that social media content must be included when responding to requests that include more general phrases such as "all notifications of the street closure" and "all emails and communications referencing the topic".

PREPAREDNESS FOR LEGAL DISCOVERY

Legal discovery costs continue to escalate in frequency and magnitude, and social media materials are increasingly requested during litigation. What many do not realize is that a failure to produce social media records during litigation often results in sanctions, fines, and a compromised legal position.

To mitigate risk and satisfy legal requirements, organizations must implement a comprehensive records management strategy that includes social media. However, social media presents a number of unique challenges related to accessing, capturing, and preserving the data.

The primary challenge is that, unlike emails and other document files, social media exists entirely outside the control of an agency's IT department. Instead, social networking providers such as Facebook and Twitter maintain full control over the social media communications on their platform and provide absolutely no guarantee to government that content will be maintained for the long term. If content is edited or deleted, records are lost forever. In fact, in its guidelines for law enforcement, Facebook specifically states, "We do not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service." The potential for data deletion is especially troubling given that citizens can easily delete past communications to government without any indication that the communication is no longer available.

Chapter 2:
MITIGATING RISK WITH AN INTERNAL SOCIAL MEDIA POLICY

The first step in addressing the issues outlined in the previous chapter is establishing an internal social media policy. The following sections detail the critical components of an internal social media policy:

PERSONAL VS PROFESSIONAL USAGE

An internal social media policy should clearly establish guidelines and boundaries for employees. Although each agency must tailor its social media policy to its own internal needs, the following are recommended employee usage provisions:

1. The policy should clearly communicate to employees whether social media use in the workplace will be prohibited, monitored, or allowed within reasonable time limits. The policy should be careful not to excessively restrict the content of employee social media postings to the extent that "protected concerted activity" among the company's employees would be prohibited. For example, a social media policy should not ban "inappropriate discussions" about the company, management, working conditions, or coworkers that would be considered protected speech in another form or forum.
2. The policy should also caution employees that they have no expectation of privacy while using the internet on employer equipment. If employees will be monitored, the policy should inform employees of such monitoring.
3. The policy might also require employees who identify themselves as employees of a particular company to post a disclaimer that any postings or blogs are solely the opinion of the employee and not the employer.
4. Employees should be advised that they should not use the company logo, seal, trademark, or other symbol without written consent of the administrator.
5. The policy should also address the protection of confidential and sensitive information, as well as personal information relating to employees or customers.
6. Finally, all employees should be required to sign a written acknowledgment that they have received, have read, understand, and agree to comply with the social media policy.

REGISTRATION OF SOCIAL MEDIA SITES

A fundamental component of the employee-use policy is the section describing approval and registration of social media sites. In many organizations, it might not be practical for a centralized communications team to publish each and every social media communication for an entire city or county. Attempting to do so can make it difficult to maintain a highly relevant and responsive social media presence. However, it can certainly be beneficial for a centralized department to approve the creation and use of each professional social media profile across the organization.

Agencies can leverage this part of the process to ensure brand consistency, provide training, and ensure that each social networking profile serves a distinct and meaningful purpose. Additionally, the approval process provides a natural entry point for populating and maintaining a registry of the organization's social media profiles.

The following excerpt from the Fairfax County, Va., Social Media Policy & Guidelines for Official Accounts offers a great example of how this protocol can fit into a social media policy:

Requesting Facebook and/or Twitter

New social media sites on Facebook and/or Twitter may be requested by first sending an e-mail to [E-mail Address]. Departments/programs may not create their own social media sites. Agencies are initially limited to one account on Facebook and/or Twitter. It's also preferred if agencies launch one platform at a time. If approved, the Office of Public Affairs will create pages with proper settings, look and feel to ensure consistency; transfer administrative rights to the agency; and provide training.

Approval and Registration of New Social Media Accounts

All Agency social media sites shall be (1) approved by [contact]; (2) published using approved social networking platform and tools; and (3) administered by the contact or their designee.

PUBLIC RECORDS & RECORDS MANAGEMENT

It is a good idea for any business to keep records of its important communications. This is especially true in government due to the legal mandate created by public records laws. These laws have been in place for many years and, as a result, governments at every level have established record retention policies and procedures. Most public entities have also invested in internal IT infrastructure to retain electronic data such as emails and files.

Record keeping serves three fundamental purposes in regards in minimizing risk for government:

- Most directly, it avoids lawsuits and fines resulting from noncompliance with public records laws.
- It ensures that valuable information is available when needed in critical business scenarios such as litigation or internal investigations.
- It establishes transparency and accountability, both internally and externally.

Unfortunately, public entities are often confused about how to apply existing record keeping

procedures and technology to social media. Social media records cannot be readily retained by IT because the communications might never have passed through the IT infrastructure. Citizens and government employees alike are leveraging a wide variety of computing devices to engage on social media, and can feasibly send and receive content without ever authenticating with the corporate network. Furthermore, the sheer volume and complexity of social media content introduces new challenges in maintaining accurate digital records.

Many public entities have adopted manual procedures such as taking screenshots and copying & pasting, but these approaches are both time consuming and ineffective. Content is rapidly shared and modified across social media and it is simply not possible for a human being to manually maintain accurate records. Furthermore, records captured manually lack authenticity—they are missing electronic record metadata, and are easy to alter.

Realistically, the sheer technical complexity of addressing requirements across a continually evolving social media landscape is likely outside the scope of the available resources of most agencies. The reality is that public entities must rely on external technology more than ever to address record keeping needs. In particular, many public entities are starting to leverage external social media archiving services to automate record keeping in a comprehensive yet cost-effective manner.

Regardless of the record keeping approach selected, an internal social media policy must advise staff regarding public records concerns and require record retention of social media content.

Chapter 3:

MITIGATING RISK WITH AN EXTERNAL SOCIAL MEDIA POLICY

COMMENT MODERATION

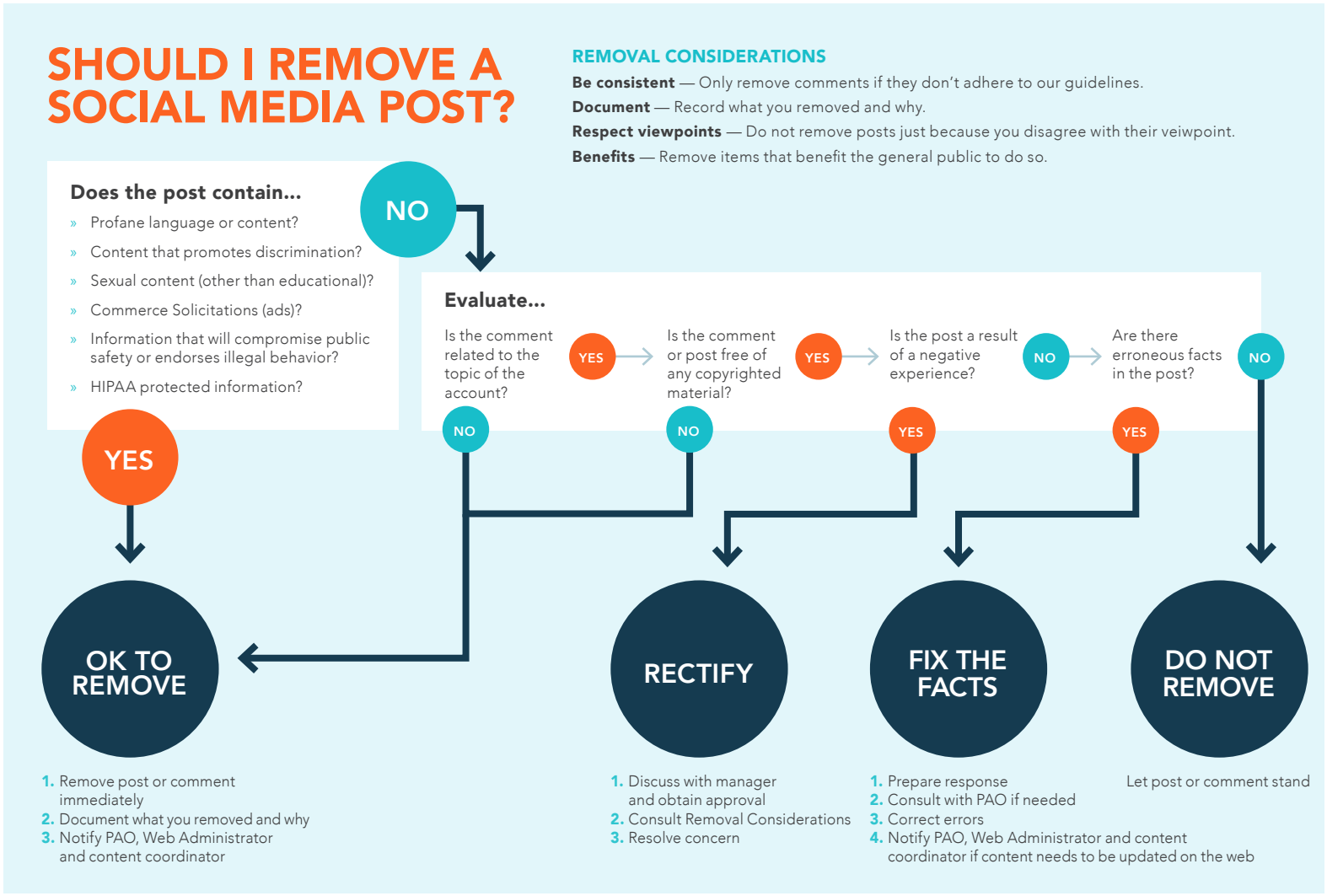
One of the most challenging practices to implement correctly in government social media usage is comment moderation. It is not wise for government bodies to remove comments, posts, or other content it doesn't like on its official social media sites in the same way a private individual, organization, or company might do. In addition to records retention issues, the removal of this content could infringe First Amendment rights and land a government entity in court—as happened to the City & County of Honolulu as detailed in Chapter 2.

Hence, when looking to moderate public comments on social media, it is necessary to develop a clear, tightly scoped policy that avoids confusion and can withstand external challenges.

To start with, certain categories of speech, including obscenity and direct threats, are not entitled to full protection under the First Amendment. Commercial speech is also subject to different treatment under the law, and can be excluded from a government page. And, of course, privacy laws can be invoked to justify the removal of personally identifiable information such as phone numbers, home addresses, and social security numbers.

Those are the easy cases, but what about the dreaded "off topic" comments? While it has yet to be tested in the highest courts, a strong case can be made that the US Supreme Court definition of a "limited public forum" can be applied to social media. Under this definition, public agencies can create designated forums in which they may limit the topic of speech or the class of speaker as long as they don't discriminate based on viewpoint.

Once a policy has been established, it is critical that internal staff is appropriately trained. For example, here is a flow chart created by Wake County, North Carolina to help staff make the appropriate decision:



Content used with permission from Wake County, North Carolina.

PUBLIC RECORDS DISCLAIMER

Since posts and comments across social media are a matter of public record, citizens must be aware that their communications are being retained and could be shared with others, even if those communications are moderated or later deleted. Similar to disclaimers on government emails, appropriate language should be used to inform the public of your external social media policy. Below is an example of an appropriate statement from a Facebook profile acknowledging public records law:

External Social Media Policy Disclaimer

Agency social media sites are subject to applicable public records laws. Any content maintained in a social media format related to agency business, including communication posted by the Agency and communication received from citizens, is a public record. The Department maintaining the site is responsible for responding completely and accurately to any public records request for social media content.

The public records disclaimers must be easily located and accessible by visitors to your social networking sites. A common practice is to include a link in the "About" section of each of your social networking profiles that directs visitors to a website containing your policy. However, space permitting, it may be worth embedding the public records disclaimer more explicitly on the social networking site to ensure that citizens are fully aware that their postings will be retained and potentially disclosed.

IMPLEMENTATION AND ENFORCEMENT OF POLICY

This section is designed to provide starting points for implementing and reinforcing an agency's social media policy.

Collaboration with IT and Communications

Legal teams must collaborate closely with communications teams and IT departments in order to ensure successful implementation of social media policy. Communications teams are intimately familiar with the nature of content transmitted and received across social media, but may need to be educated in regards to legal imperatives such as records retention. IT departments are often responsible for evaluating vendors and technology solutions, but must understand the legal implications and the reasons for implementing solutions proactively.

Below is an example step-by-step process for engaging these stakeholders:

- **Step 1: Kickoff** *(Legal + IT + Communications)* Set expectations for reviewing or setting in place policies and safeguards for the agency's social media. Review example scenarios and case law to help clarify the need for action.
- **Step 2: Assessment** *(Legal + Communications)* Conduct an assessment of the agency's social media accounts in order to clarify business use cases and identify potential risk areas.
- **Step 3: Policy Review** *(Legal + Communications)* Evaluate your current internal and external policies for social media to ensure appropriate legal coverage based on the assessment conducted in Step 2.
- **Step 4: Technology Review** *(Legal + IT)* Evaluate account management and record retention procedures to determine if additional technology is required.
- **Step 5: Recommendations** *(Legal + IT + Communications)* Establish a recommendations plan to shore up any gaps that exist with the agency's use of social media. This may involve adjustments to both the internal and external policy, improved education for internal staff, evaluation of additional archiving technology, and more.
- **Step 6: Implement and Validate** *(Legal + IT + Communications)* Implement the recommendations identified in Step 5 and perform a final assessment to ensure that the the issues identified in Step 3 and Step 4 are fully addressed.

It is a best practice to repeat this process annually as new social media platforms and legal precedents emerge.

Conclusion:
LEGAL CHECKLIST FOR MITIGATING SOCIAL MEDIA RISK

There is no doubt that social media will continue to have a growing role within government operations and will expand into many exciting and unexpected areas of practice. As new social media tools and case law redefine the legal landscape, it is vital to have strategies and policies in place today to mitigate new risks. No matter the state of social media use in your agency, we encourage you to use this guide as a reference for your programs. The checklist below can help you manage the process of implementing the necessary policy and technology to protect your agency. Finally, we invite you to share your stories of success and lessons learned for future evolutions of this guide.

SOCIAL MEDIA RISK MITIGATION CHECKLIST

Understand your current social media landscape

- ☐ **Conduct** a social media inventory of each social media account your agency is using
- ☐ **Identify** who is responsible for each account and identify a backup person in the event the primary contact is out-of-office
- ☐ **Identify** any existing policies or internal procedures that have been adopted to cover social media usage

Implement or revise your internal social media policy

- ☐ **Clarify** personal vs professional usage
- ☐ **Require** approval and registration of corporate social networking profiles
- ☐ **Avoid** collecting personal login credentials for social networking profiles
- ☐ **Ensure** the agency maintains ownership and access to all social networking profiles
- ☐ **Pursue** verified status indicators where possible for each social networking profile
- ☐ **Require** records management and retention of social media content in accordance with public records requirements
- ☐ **Conduct** staff training

Implement or revise your external social media policy

- ☐ **Define** comment moderation guidelines
- ☐ **Provide** an easily accessible link to the full policy on all social networking profiles
- ☐ **Ensure** a public records disclaimer is prominently displayed on all social networking profiles
- ☐ **Conduct** staff training

Implement or revise records management procedures

- ☐ **Educate** staff regarding public records requirements
- ☐ **Evaluate** and implement social media archiving technologies
- ☐ **Require** archiving of all social networking profiles that communicate in relation to the business of the agency
- ☐ **Develop** a protocol for integrating social media content in response to records requests and legal discovery requests

ENDNOTES

1. Hispanics United of Buffalo, Inc., 359 NLRB No. 37 (Dec. 14, 2012).
2. NLRB Case #28-CA-023267 Lee Enterprises, Inc. d/b/a Arizona Daily Star https://www.nlrb.gov/case/28-CA-023267
3. Page v. Lexington County School District One, No. 07-1697. (June 23, 2008)
4. Karras v. County of San Diego, No. 3:2014cv02564 (October 27, 2014)
5. Hawaii Defense Foundation, et al. v. City and County of Honolulu, et al., No. 1:2012-cv-00469 (D. Haw. filed Aug. 21, 2012).