Social Media & Municipalities - Legal & Ethical Issues

Julie A. Tappendorf
Ancel Glink Diamond Bush DiCianni & Krafthefer, P.C.

I. INTRODUCTION

Social networking describes a new set of Internet tools that enable shared community experiences, both online and in person. These sites go beyond the more "passive" websites operated by governments and organizations. Each of the various social networking sites is tailored to a specific need and is designed to encourage active participation by both the member and his or her audience. For example, "Linked In" is marketed to businesses and professionals as a way to interact and form networks or "connections" with others. Facebook enables users to create a profile, update a status, include pictures, add "friends," and post comments on the "walls" of personal or friend pages. Twitter allows people to connect with (or "follow") a large number of users and post short notes of no more than 140 characters, called "tweets." Flikr and YouTube allow users to post photos or videos, respectively, to share with others.

The growth of social media applications in the government context has an impact not only on government officials who use social media, but also the increasingly information-hungry general public, who expect local, state, and even the federal government to use these technologies to more effectively disseminate information and allow a forum for comment. In fact, social media provide the public sector a wealth of opportunity to communicate with the public, with interested stakeholders, and with each other about new proposals and ideas. Additionally, social media may be used by all parties interested in public sector decision making, including developers, applicants, individual advocates, non-profit organizations, or governmental entities.

However, the general benefits of the use of these new technologies—which include the promise of greater transparency and greater public participation—must be weighed against the potential drawbacks, such as truthfulness and accuracy of posted information, the source of the posted information, and the longevity of inaccurate information in cyberspace. Additionally, there are a number of issues to consider when public officials and employees choose to utilize social networking tools, as well as a host of legal issues when organizations choose to create and host these sites.

II. LEGAL ISSUES

Despite the growth and overall positive reports of how the public sector has embraced social media, there are a growing number of legal issues that governments will face in their use of social media.

A. Open Meetings Act

The policy behind the Open Meetings Act is that government decision-making and legislation should be made openly, and not in secret or closed-door session, so that the general public can be fully informed and provide input regarding the proposed actions of the decision-making body. To this end, the Open Meetings Act requires that all meetings of decision-making bodies provide notice and be open to the public (with certain statutorily provided exceptions).

Communications which take place on a social media platform have the potential to run afoul of open meeting laws. Without realizing it, these communications: "friending," "tweeting," "messaging," "blogging—all considered informal by most people's standards—can constitute a "meeting" under most open meeting law regimes.

Because of the "newness" of social networking by government officials, there is little guidance from the courts. The Florida Attorney General, however, has issued an opinion that a government social media site would likely implicate the state open meetings requirements, among other sunshine laws. Given the potential for criminal penalties in some states' open meetings laws, government officials should be advised to avoid contemporaneous discussions or debates of public business (such as the benefits or impacts of a particular development proposal) on social networking sites or in chat rooms, and should ensure that their social networking interactions comply with applicable open meetings laws.

B. Freedom of Information Act and Records Retention Laws

Communication via a government-sponsored or maintained website or social media site (including comments and other postings) is likely to be subject to public records laws if it concerns government business. While the Freedom of Information laws may not specifically mention social media records, some states that have encountered this issue have determined that these records are subject to FOIA. For example, the Florida Attorney General has opined that information on a government social networking site would be subject to public disclosure and records retention laws if the information was made or received in connection with the transaction of official business by or on behalf of the public agency. Thus, governments must be aware that state law may require that these records be retained indefinitely or that permission must be sought prior to destroying them under public records law, and that the records must often be provided upon request. A good rule of thumb is that governments should avoid creating new material on social networking sites and instead use existing material that is already maintained for local records law compliance.

C. First Amendment

One of the most useful features of social media is the ability for interaction between the public and the government. However, this interactive aspect can quickly become a potential minefield of legal issues for public sector employees, particularly where comments and speech are involved. As this area of law is yet undeveloped, the public sector should proceed, if at all, with caution so as to avoid running afoul of the First Amendment.

Whether a site is considered a public forum (or a limited public forum) is an open question, raising concerns as to whether a government can remove allegedly objectionable Facebook comments without implicating First Amendment protections. The issue of whether social media is a public forum may be answered sooner rather than later as a case of first impression was filed last fall in a Honolulu court. In that case, *Hawaii Defense Foundation v. City and County of Honolulu*, various individuals and a non-profit organization filed a lawsuit against Honolulu because comments critical to the City's police department had been routinely removed from the City's Facebook page. The plaintiffs argue that the City had created a traditional public forum when it established a Facebook page and opened it up to public comments. This case is worth watching as it appears to be the first of its kind in this area of law.

Other legal issues may arise in allowing persons to post comments and other information on local

government social networking sites, such as revealing confidential or proprietary company information.

By completely restricting the general public's ability to comment and communicate through a social media page or website, a governmental agency has created a nonpublic forum and the agency is not liable for First Amendment repercussions so long as its restrictions on the content of the site are viewpoint neutral (if the government allows an issue to be presented, it cannot limit the presentation to only one view), and reasonably related to a legitimate government purpose.

However, if the government agency does allow others to comment or post information on a social media page, a designated public forum has arguably been made. If a designated public forum were created, then the organization cannot exclude or delete material based on its content unless the restriction is "narrowly drawn to effectuate a compelling state interest" -- content-neutral restrictions can be placed on comments so long as they are narrowly tailored, serve a significant government interest, and leaves open alternative channels of communication.

On the other hand, if a government only allows certain groups to comment on certain topics, it has probably created a limited public forum. This would likely be the case for agencies who maintain a certain type of Facebook page, where the public user can only post comments after "friending" or "liking" the agencies page. In a limited public forum, a government entity can restrict comments as long as these restrictions are reasonable and viewpoint neutral. Governments that moderate comments and remove those that are objectionable should be careful to remove only content that is vulgar, completely out of context, or that targets or disparages any ethnic, racial, or religious group. Content that is simply politically unfavorable or negative in the context of the conversation should be allowed to remain. The more a social media platform mirrors a public meeting (e.g., the more participatory it becomes), the stronger the case a government entity has in upholding its restrictions, as government entity meetings have been found to be a limited public forum.

D. Discrimination

Governments who use social media must be aware of, and address the fact that some people are unable to access the Internet for a variety of reasons. Although this can stem from many situations, governmental agencies need to make sure that they are not using social media, as well as the Internet, in a manner that actually hampers the access of information from certain subset groups of people.

A variety of statutes affect governmental agencies which use social media, including the Americans with Disabilities Act and the Rehabilitation Act. Government bodies are obligated by law to provide disabled individuals with "equal access" to information posted on social networking sites, unless it would "pose an undue burden" or that doing so would "fundamentally alter the nature of the provider's programs." Thus, governments who use social networking sites should have an alternative way to provide the information to disabled individuals, such as sending it through the mail or reporting it by phone.

Furthermore, governmental agencies must also take care not to overuse social media, and perhaps incidentally alienate segments of the populations which do not traditionally use social media. Data shows that there is a discrepancy in the use of the Internet by income, race, age, and education level, raising concerns that the use of social networks to share information and solicit input on government issues and projects might reach a less diverse group of people. If government officials

are using social networking sites as the only means to get information and receive input, a significant number of citizens may be underrepresented.

E. Copyright Issues

Governmental entities also need to be careful about what they post on social media pages to avoid potential copyright liability, as well as protect their own original work-product. Photos and video should be produced by the organization or individual who posts the media. If copyrighted materials are used, the poster should make sure it obtains and maintains physical records of the copyright licenses. All users of social media sites should also be aware that some social networking sites (such as Facebook) have terms of use in place that state that by posting intellectual property on Facebook, an individual grants Facebook a "non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content" that is posted. Consequently, users should be cautious and sensitive to the content uploaded on these sites.

F. Privacy

Many social media platforms allow users to set their own privacy settings, which often cover a number of areas including who view their profile, who can post comments and other content on the profile, and who can search for their social media page or channel. Although the vast majority of these privacy concerns apply to individual users, public sector users should be equally as conscious. Everyone who uses social media should begin with the assumption that everything posted on a government site is likely a public record. Privacy issues involving social media are being slowly developed through case-law, and are still considered an open question subject to further explanation.

Also, be aware that if a governmental entity requires people to register to use a government social networking site, it must carefully consider what information the registrant must provide (name, address, phone number, email, screen name), who will maintain the information, and whether others participating in the discussion will have access to this information.

III. EMPLOYEE USE OF SOCIAL MEDIA

Public employers continue to walk a tightrope when regulating the use and content of the electronic communications of its employees and when taking employment action based on the use or content of its employees' electronic communications. The law is well settled that a public employee has a limited or no expectation of privacy in their office, desk, locker or even their telephone calls at work. Unfortunately, the law moves slowly and is far from addressing the balance of rights of employees and employers in the context of electronic communications.

A. Constitutional Protections

Public employees do not surrender all of their First Amendment rights, particularly their speech rights, merely because they are employed by the government. However, the speech of public employees can be subject to certain restrictions by the government, because it has a different—and more significant—interest in regulating the speech of its employees than the general public.

The U.S. Supreme Court has outlined a two step analysis for determining whether the speech of public employees is protected by the First Amendment. First, it must be determined whether the

employee spoke as a citizen on a "matter of public concern." If the speech is a matter of public concern, then the court must engage in the *Pickering* balancing and decide whether the government was justified for treating the employee's speech differently from the general public.

Courts decide whether speech is a matter of public concern based on "the content, form, and context of a given statement, as revealed by the whole record." Of these three factors, the content of the statements have generally been acknowledged to be the most important, although the form and context can help make a statement one of public concern if the speech at issue occurs in an unconfined space. Matters which have been found to be of the public concern include: speech relating to public safety and policy protection; governmental wrongdoing and misconduct; or speech which seeks to expose wrongdoing by government officials.

Pickering balancing has been used in Internet postings. In *Curran v. Cousins*, 509 F.3d 36, 49 (1st Cir. 2007), a corrections officer was terminated for postings he made on a union website. This website was owned and controlled completely separately from the public employer, and featured a public discussion board which allowed registered users to "post comments and statements. Any person with access to the Internet—whether a member of the union or not—could register, post, and read messages." The officer, who had been suspended a week earlier for "threatening and menacing" co-workers, posted messages to the website that made unfavorably comparisons to the current sheriff, and his personnel decision-making to Adolf Hitler and the Nazis during World War II. The employee was thereafter fired due, in part, to his posting on the website. The First Circuit did note that although most of the content of the posting was not a matter of public concern, a part of the posting which addressed the sheriff making personnel decisions based on political affiliations rather than merit was a matter of public concern. However, in balancing the speech of the employee and the later actions of his employer to fire him, the court found that the government was plainly justified in firing the employee. In the posting, the employee referenced the plot of Hitler's generals to kill him, and urged a similar plot by analogizing the current sheriff to Hitler. Further, the court found that "[s]peech done in a vulgar, insulting, and defiant manner is entitled to less weight in the *Pickering* balance."

B. Hiring Decisions

Never has so much information about so many been available with the click of a mouse. Every prospective employer is interested to know everything that they can about a job applicant. And every employer knows that they might find something on the Internet which the applicant is reluctant to divulge in an interview. It may not be a matter of finding out "dirt" on the candidate, but just learning more about their likes, dislikes, lifestyle, thoughts and beliefs which may provide greater insight into their potential suitability as an employee. Nevertheless, the question arises as to what information from the Internet an employer can use when making hiring decisions.

Reliance on Internet information has become so common that we often forget that not all information obtained in Internet searches is completely accurate. Anyone can post information on the Internet and no assurance exists that it is all truthful. We have all heard about altered photos and intentionally planted misinformation which causes problems for an individual, to say nothing of the problems of those with common names or the same name as someone with a negative reputation. If searching for information on job candidates on the Internet, always remember that the information may not be truthful, accurate or reliable.

While it is not illegal to review public information about job candidates, it is advisable that candidates know of this possibility ahead of time. If candidates are aware that searches of social network and other Internet sites is part of the candidate review process, a decision based in whole or part on this information will not be inconsistent with their expectations. Thus, they will be less likely to claim that an adverse decision was the product of discrimination or other illegal basis.

Prospective employers can make employment decisions on any basis that is not illegal. Examples of illegal considerations are those such as race, gender, and religion. Off duty conduct can be a relevant job qualification depending on the position for which the employee applies. For example, it may be relevant to the qualifications of a police officer whether that individual posts pictures of him or herself in situations which depict illegal activity. Evidence of gang affiliation may also disqualify a candidate from employment with law enforcement. Whether information gathered from electronic sources, or any other, serves to disqualify a candidate from public employment depends largely on the position which is sought and the type of behavior which is disclosed. On the other hand, public employers must take great care to avoid decisions based on social network information related to religious affiliation, ethnic or racial information gathered only from these searches and other information which, if used, as a basis to deny employment would violate the law.

Finally, given the potential for inaccurate information gathered from social networks or other Internet sites, it is advisable to allow a candidate to provide explanation to any information gathered from these sources to ensure that a decision is not based on false information.

C. Discipline of Current Employees

Evidence of misconduct related to work performance that is gathered from social network sites may be an appropriate basis for action against current employees. Like pre-employment considerations, 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. So, for example, the police officer or teacher who posts obscene pictures of himself or herself on their Facebook page, or photos of obvious illegal conduct, likely serves an appropriate basis for disciplinary action.

Local government employers, like other bosses, are struggling with critical social media posts by employees. 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? The answers to these questions are not yet clear, because there is little case law on this issue. However, the National Labor Relations Board (NLRB) has been active in this area recently. While the National Labor Relations Act does not apply to local government employees, the NLRB rulings can provide government employers with some guidance.

In one case, the NLRB ruled that an employer unlawfully discharged five employees who 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. The NLRB cited the *Meyers* ruling that an activity is concerted when an employee acts "with or on the authority of other employees, and not solely by and on behalf of the employee himself." In this case, the discussion was initiated by one worker in an appeal to her coworkers on the issue of job performance, resulting in a "conversation" on Facebok among coworkers about job performance. The NLRB ruled similarly in a number of other cases.

In another case, 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 and began posting news stories. A week after the employee posted a tweet critical of the newspaper's copy editors, the newspaper informed the employee he was prohibited from airing his grievances or commenting about the newspaper on social media. The reporter continued to tweet, including posts about homicides in the City and a post that criticized an area television station. 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 the conditions of employment and (2) did not seek to involve other employees on issues related to employment. The NLRB issued a similar ruling in a case involving a bartender who posted a Facebook message critical of the employer's tipping policy, finding the posts mere "gripes" that are not protected.

Two recurring themes have come out of recent NLRB rulings. First, individual gripes or venting by employees is not protected, and employers can discipline, and even terminate, employees for this conduct. Second, the NLRB is taking a very narrow view of social media policies and striking down policies for being overbroad where they could be interpreted to prohibit protected conduct.

What does this mean for local government 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 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.

D. Employer Requests for Social Media Passwords.

It has become common practice for public and private employers to review the publicly available Facebook, Twitter and other social networking sites of job applicants as part of the vetting of candidates 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 are asking candidates to either turn over their passwords or log on to their social media accounts during the interview.

Because an applicant can decide not to apply for a particular job, some employers have argued that it is neither an invasion of privacy nor a violation of constitutional rights to ask for this information during the hiring process and if applicants refuse to provide the requested information, employers are free to drop their consideration for hire. Nevertheless, the ACLU and others argue that this practice violates a candidate's right to privacy.

Until recently, there was no federal or state law expressly prohibiting this practice, although a few states have proposed or enacted legislation. Maryland became the first state to pass a law on the practice in April. Two identical bills, S.B. 433 and H.B. 964, were passed by the state legislature, and signed by the Governor into law. Under this new law, employers are prohibited from requiring employees and job applicants to “disclose any user name, password, or other means for accessing a personal account or service” electronically. Employers are also prohibited from refusing to hire an applicant for not providing access to this information. Similarly, employers are not permitted to terminate or discipline an employee for refusing to provide this information.

In addition to protecting the privacy of current and prospective employees, the Maryland law also provides employers with some protections. For example, employees are prohibited from downloading "unauthorized employer proprietary information or financial data" to personal accounts or to websites, and the law allows employers to investigate these activities to ensure "compliance with applicable securities or financial law or regulatory requirements." Additionally, employers are permitted to require employees to provide passwords and login information for non-personal accounts that are part of the employer's own systems, such as company e-mail accounts. The Maryland law took effect October 1, 2012.

The second state to pass a similar law is Illinois. Illinois P.A. 97-0875 prohibits public employers from seeking job applicants' social media passwords. The legislation 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. The new law became effective January 1, 2013. Ten states have enacted or proposed legislation similar to the Illinois and Maryland laws.

Employers should be cautious in using social media to discipline current employees. 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 usage and the employee's right to hold their job.

IV. ETHICS AND USE OF SOCIAL MEDIA BY ATTORNEYS

An American Bar Association study found that more than half of lawyers are members of at least one social networking site. Lawyers and law firms benefit from social media sites for the same reasons other businesses benefit – the dissemination of information about the firm and its attorneys and marketing the firm and its attorneys to potential clients. Many of the same legal issues that apply to government entities, organizations, and private companies also apply to lawyers and law firms, including copyright concerns, employment usage, among others.

While social media use is relatively new for lawyers and law firms, there have already been a number of ethical issues that have arisen from attorney use of social networking. Since each jurisdiction has its own ethical rules in place for attorneys practicing in the state, it is important to consult applicable rules and opinions of the practicing jurisdiction. However, a general discussion of the types of ethical issues that have arisen in the field of social media use by attorneys may be helpful to provide some guidance on these issues.

A. Solicitation and Advertising

A lawyer may advertise services through written, recorded, or electronic communication, including public media. However, a comment to ABA Model Rule 7.2 cautions against real-time electronic solicitation of prospective clients. Thus, emails are probably acceptable, but not instant messaging or participation in chat rooms. Other forms of online solicitation may also be a violation of the prohibition of in-person, telephonic, or real time electronic solicitation.

B. Practice and Specialization

A lawyer may not mislead or misrepresent his or her practice nor may a lawyer state or imply that he or she is certified as a specialist in a particular field of law. Lawyers should avoid providing legal advice in areas of the law where they are not experienced and should be careful not to misrepresent

their practice area expertise and experience. In addition, some jurisdictions prohibit attorneys from self-identifying as an "expert" or "specialist" in a particular field of law. This rule can be tricky to follow on certain social media sites, such as LinkedIn, that ask for "specializations" in their profile forms, and allow users to "endorse" other users' skills and expertise.

C. Jurisdiction

Lawyers are only authorized to practice in jurisdictions where they are licensed. Social media sites, blogs, listservs, and similar sites can make this difficult for an attorney with exposure to people across the country looking to the attorney for guidance on state-specific legal issues. A lawyer should be careful not to provide legal advice on these state-specific legal issues unless he or she is licensed in that particular jurisdiction.

D. Attorney-Client Relationship

Just as attorneys must be careful not to inadvertently create an attorney-client relationship at a cocktail party, over the telephone, on an airplane, by email, and through a law firm's "question and answer" page on its website, attorneys must also be careful not to create an attorney-client relationship when using social networking sites. An attorney-client relationship might be formed when an individual "reasonably relies" on an attorney's advice through a blog entry, listserv, or social networking site.

E. *Ex Parte* Communications

Lawyers should be aware that judges also participate in social networking and may have access to a lawyer's communications that might implicate the prohibition on *ex parte* communications on pending matters. For example, listservs may have thousands of participants and a harmless "inquiry" about a pending matter could be read by the judge who is assigned to that pending matter.

F. Contact with Witnesses and Represented Parties

Social media can provide lawyers with a bonanza of valuable personal information from other users, which, in turn, lawyers can use when preparing for litigation or settlement discussions. This can lead to many ethical complications which lawyers may not anticipate during their investigations. When using social media to investigate another party, lawyers must be careful not to engage in deceitful behavior, such as asking a paralegal or co-workers' to use their account to gain access to information about that witness. The Philadelphia, San Diego County, and New York City Bars have all issued opinions to place restrictions on lawyers seeking to "friend" potential witnesses.

Even when a lawyer uses their true identity to "friend" or follow another party through social media even more ethical concerns can arise. Ethical rules place restrictions on the communications lawyers make with third parties who are represented by counsel. For example, a lawyer cannot communicate about the proceeding with a represented party unless they have the consent of that party's lawyer or a court order. This is the case even if the person consents to the communication—i.e., even if they accept, respond, or engage any friend requests or messages sent.

V. IMPORTANCE OF A SOCIAL MEDIA POLICY

Governments (and law firms for that matter) that participate in social networking sites must start

with the realization that what is posted on social networking sites is public information. That means that employees and officers should not post information that neither they nor the employer would want everyone to know. By realizing the public nature of the information being published, confusion, lawsuits, and other problems can be more easily avoided.

All governments that use any form of online communication should develop, implement, and enforce a website and social networking policy. That policy should include a well-defined purpose and scope for using social media, identify a moderator in charge of the site, develop standards for appropriate public interaction and posting of comments, establish guidelines for record retention and compliance with public records and meetings laws, and include an employee access and use policy. The government should also post express disclaimers on its websites reserving the right to delete submissions that contain vulgar language, personal attacks of any kind, or offensive comments that target or disparage any ethnic, racial, or religious group. Finally, the employer should train employees regarding appropriate use of social networking and how use might impact the employer.

In crafting a social media policy, an employer should be careful not to implicate the First Amendment rights of its employees nor violate any applicable federal or state employment laws protecting employees. An example of this type of situation involved a settlement between the National Labor Relations Board and an ambulance service in Connecticut that fired an employee in 2009 for venting about her boss on Facebook. The ambulance company argued that the employee's Facebook criticism violated the company's social media policy barring workers from disparaging the company or their supervisors. The NLRB argued that the National Labor Relations Act protects an employee's discussion of conditions of his or her employment with others and that co-workers comments on the employee's Facebook page implicated those protections. As part of the settlement, the company stated it would change its policy so it did not restrict employees from discussing work and working conditions when they are not on the job.

As discussed previously, the NLRB has struck down a number of social media policies for being too broad, so it is recommended that employers take care in crafting a social media policy that avoids these issues.

A government might also consider providing examples of acceptable or unacceptable conduct in both employee and public usage of social media to illustrate the type of conduct that is regulated and why a particular regulation is in place.

Finally, all employees should be required to sign a written acknowledgement that they have received, read, understand, and agree to comply with the social media policy.

A checklist for drafting a social media policy can be found on Appendix A, and a sample employee acknowledgement form that can be used in connection with the adoption of a social media policy is attached as Appendix B. In addition, a copy of a social media policy that was upheld by the NLRB is attached as Appendix C. Please note that this policy was not adopted by a government entity, so many of the issues discussed in this outline (i.e., Open Meetings, FOIA, and First Amendment) are not covered by this policy, but are recommended to be included in a government social media policy.

Appendix A

Checklist for Drafting a Social Media Policy

A local government considering establishing a community Facebook, Twitter, or other social networking site should first adopt a social media policy to govern the administration and monitoring of site content, set ground rules for public input and comments, and adopt policies for employee usage of social media.

1. Purpose

The policy should contain a statement that the use of social media by the government entity is for the purpose of obtaining or conveying information that is useful to, or will further the goals of, the government.

2. Approval and Administration

The policy should provide for an administrator to oversee and supervise the social media networking sites of the government. The administrator should be trained regarding the terms of the policy and his other responsibilities to review content to ensure that it complies with the policy and furthers the government's goals.

3. Comment Policy

The policy should identify the type of content that is not permitted on a social media site and that is subject to removal. This might include comments that are not relevant to the original topic; profane, obscene, or violent content; discriminatory content; threats; solicitation of business; content that violates a copyright or trademark; and any content in violation of federal, state, or local law. The policy should also contain a disclaimer that any comment posted by a member of the public is not the opinion of the government. Finally, the policy should include language that reserves the right of the administrator to remove content that violates the policy or any applicable law.

4. Compliance with Laws

The policy should include language regarding compliance with applicable federal, state, and local laws, regulations, and policies. It should be made clear that content posted on a government site is subject to freedom of information and record retention laws. In addition, content posted on social media sites may be subject to e-discovery laws. Finally, information that is protected by copyright or trademark should not be posted or maintained on a social media site unless the owner of the intellectual property has granted permission.

5. Employee Usage Policy

A social media policy should clearly establish guidelines and boundaries to enable employees to anticipate and understand company expectations and restrictions regarding social media usage. Although each employer should create a social media policy tailored to the particular employer's workplace, the following are some suggested employee usage provisions:

a. 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.

b. 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.

c. The policy might also require employees who identify themselves as employees of a particular government or company to post a disclaimer that any postings or blogs are solely the opinion of the employee and not the employer.

d. Employees should be advised that they should not use the government or company logo, seal, trademark, or other symbol without written consent of the administrator.

e. The policy should also address the protection of confidential and sensitive government information, as well as personal information relating to government officials and employees, customers, or residents.

f. Prior to taking any adverse employment action against an employee on account of the content of the employee's social media posting, consider whether the employee's comments (1) were posted on a public site accessible to a large number of people; (2) disclosed confidential information about the employer, its employees, residents, or others; or (3) were directed at coworkers in a serious effort to discuss working conditions or were simply a venue for the employee to vent personal frustration. Any decision to take adverse employment action against an employee on account of social media use should be made in consultation with legal counsel.

g. 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 (see e.g., Appendix B).

h. Appendix B

Employee Acknowledgment Form

I acknowledge that I have received a copy of the [Employer Name] Social Media Policy dated [date].

I understand that this policy replaces any and all prior verbal and written communications regarding [Employer Name] policies relating to employee use and access and employer monitoring of employee use of social media, as defined in the social media policy.

I have read and understand the contents of the social media policy and will act in accord with these policies and procedures as a condition of my employment with [Employer Name].

I understand that if I have questions or concerns at any time about the social media policy, I will consult my immediate supervisor, my supervisor's manager, the Human Resources Department, or the head of the [Employer Name] for clarification.

Finally, I understand that the contents of the social media policy may change at any time.

Please read this social media policy carefully before you sign this document.

_____

Employee Signature

_____

Date

_____

Employee Name (Please Print)

Appendix C

NLRB-Approved Social Media Policy

Social Media Policy
Updated: May 4, 2012

At [Employer], we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

This policy applies to all associates who work for [Employer], or one of its subsidiary companies in the United States ([Employer]).

Managers and supervisors should use the supplemental Social Media Management Guidelines for additional guidance in administering the policy.

GUIDELINES

In the rapidly expanding world of electronic communications, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with [Employer], as well as any other form of electronic communication.

The same principles and guidelines found in [Employer] policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance , the performance of fellow associates or otherwise adversely affects members, customers, suppliers, people who work on behalf of [Employer] or [Employer's] legitimate business interests may result in disciplinary action up to and including termination.

KNOW AND FOLLOW THE RULES

Carefully read these guidelines, the [Employer] Statement of Ethics Policy, the [Employer] Information Policy and the Discrimination & Harassment Prevention Policy, and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence of similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

BE RESPECTFUL

Always be fair and courteous to fellow associates, customers, members, suppliers or people who work on behalf of [Employer]. Also, keep in mind that you are more likely to resolved [*sic*] work-related complaints by speaking directly with your co-workers or by utilizing our Open Door Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints

or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

BE HONEST AND ACCURATE

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about [Employer], fellow associates, members, customers, suppliers, people working on behalf of [Employer] or competitors.

POST ONLY APPROPRIATE AND RESPECTFUL CONTENT

Maintain the confidentiality of [Employer] trade secrets and private or confidential information. Trades [*sic*] secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

Respect financial information disclosure laws. It is illegal to communicate or give a "tip" on inside information to others so that they may buy or sell stocks or securities. Such online conduct may also violate the Insider Trading Policy.

Do not create a link from your blog, website or other social networking site to a [Employer] website without identifying yourself as a [Employer] associate.

Express only your personal opinions. Never represent yourself as a spokesperson for [Employer]. If [Employer] is a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of [Employer], fellow associates, members, customers, suppliers or people working on behalf of [Employer]. If you do publish a blog or post online related to the work you do or subjects associated with [Employer], make it clear that you are not speaking on behalf of [Employer]. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of [Employer]."

USING SOCIAL MEDIA AT WORK

Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with the Company Equipment Policy. Do not use [Employer] e-mail addresses to register on social networks, blogs, or other online tools utilized for personal use.

RETALIATION IS PROHIBITED

[Employer] prohibits taking negative action against any associate for reporting a possible deviation from this policy or for cooperating in an investigation. Any associate who retaliates against another associate for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

MEDIA CONTACTS

Associates should not speak to the media on [Employer's] behalf without contacting the Corporate Affairs Department. All media inquiries should be directed to them.

For more information

If you have questions or need further guidance, please contact your HR representative.

JULIE A. TAPPENDORF is a partner with Ancel, Glink, Diamond, Bush, DiCianni & Krafthefer, P.C. in Chicago. She practices in the area of local government, land use, and zoning litigation. Julie is a frequent speaker at local and national conferences on issues such as social networking by government bodies, sunshine laws, ethics, and a variety of land use topics. Julie has also published on a variety of local government issues, including a land use casebook, books on development agreements and exactions, and chapters and articles on social media, annexation and subdivisions, and regulating distressed properties. The American Bar Association recently published a book she co-authored titled Social Media and Local Governments: Navigating the New Public Square (ABA Press, 2013).

Julie currently serves as Village Attorney for the Villages of Gilberts, Lindenhurst, and Wadsworth and counsel to the Glencoe Police Pension Fund. She is an Adjunct Professor at The John Marshall Law School. Julie earned her J.D. from the University of Hawaii and her B.A. from Illinois State University. Prior to her law career, she served in the U.S. Army, Military Intelligence Branch, as a Korean cryptologic-linguist.

Julie is the author and moderator of two blogs, the local government blog Municipal Minute and the social media blog Strategically Social.

Julie A. Tappendorf, Partner
Ancel, Glink, Diamond, Bush, DiCianni & Krafthefer, P.C.
140 South Dearborn Street, 6th Floor
Chicago, IL 60603
Phone: 312-604-9182
Email: jtappendorf@ancelglink.com
Website: http://www.ancelglink.com
Blogs: http://municipalminute.ancelglink.com, http://strategicallysocial.blogspot.com