Developing Policies for Responsible Social Media Use

Having a social media policy can ensure that government employees utilize social media as a tool and not a distraction.

Heather Kerrigan | March 9, 2011

South Dakota's Secretary of State, Jason Gant, is a recent entrant into the social media world. Last month, his office joined Facebook, Twitter, and YouTube after recognizing that the state leads the nation in per-capita Facebook use (according to one social media consultant), and that social media could be helpful in getting information to citizens.

Setting up these accounts is easy, especially now that the National Association of State Chief Information Officers (NASCIO) and the National Association of Attorneys General (NAAG) have worked and are working with social media platforms to alleviate any legal barriers governments face in using social media. But once online, what government officials should and should not say or do is less clear.

Arguably, governments can't tweet or update the same way private citizens can. But the conversational manner of social media means that governments need to adapt their messages to an extent. Toeing the line between chatty and professional is tricky. Imagine the potential backlash if a government employee blurred the lines between his or her personal and professional online presences, published classified information or spouted off on a private citizen's comment on an official state or agency Facebook page. Existing personnel policies, IT access issues and the growing ability to access social media sites on the job (hello, smartphones!) makes addressing social media use tricky.

Without too many long-standing policies or guidelines governing social media use, states are starting to recognize the need to put into writing what employees can and cannot do on social media platforms. One way they are doing this is by looking to see what others are doing. I spoke with Gant and a number of officials in different states to see what policies and guidelines they created and what they address.

North Carolina and Utah created some of the first statewide social media policies in 2009. Both policies, like many around the country, address what information government officials should post. Utah's four pages of guidelines give suggestions for creating content that is valuable for citizens. This includes avoiding overly composed language and encouraging personality in posts. "Share with the participants the things we are learning and doing, and open up social media channels to learn from others," the guidelines say.

North Carolina's nine-page policy outlines what employees can say and what to do if citizen comments become offensive or off topic. When a representative of the state posts on a social media site, that person is "encouraged to be professional in their posts and to assume what is posted cannot be 'taken back,'" says Ben Niolet, director of new media in Gov. Bev Perdue's office. And as far as moderating the comments posted by citizens, agencies are encouraged to use a very light hand. "Profanity or similarly inappropriate content is typically deleted after it has been archived. Occasionally, interest groups will bombard a site with messages, a sort of virtual sit-in. Decisions on how to handle these incidents are made on a case-by-case basis," says Niolet.

Back in South Dakota, Gant wanted to align social media usage with agency goals, including transparency and openness. "We wanted people to feel comfortable posting different things and different feelings and interpretations of activities the office is engaged in," says Gant. "But we wanted to be careful that it didn't turn into information being posted that wasn't appropriate."

As a result, the South Dakota Secretary of State's social media policy was driven by "the best amalgamation of those policies as it applied to South Dakota," says Pat Powers, director of operations in the Secretary of State's office. The policy emphasizes why the office is using social media, ethics to follow, when employees can use

social media and how they can address citizen comments.

Once a state or agency has the policies or guidelines in place and participants chosen, the new rules are spread to employees by "social media delegates" or another state representative. It falls to these representatives to drum up excitement and compliance. "We had a number of meetings about what our objectives were ... and everyone's really excited about what we're doing," says Gant.

Having policies in place that govern social media use makes employees responsible for what they say and do, and also gives agencies a course of action if someone violates the privilege of access. According to a majority of state officials I spoke with, including those from South Dakota, employees are punished in accordance with existing personnel policy if a problem does arise.

Sometimes these problems revolve around personal use of social media -- both on and off the clock. Some states aren't addressing personal use of social media in their policies and guidelines because they feel that existing personnel policy drives how an employee behaves outside of the office and how that can reflect on the state. Others are adding a simple sentence into the social media policy and guidelines. States like North Carolina, Oklahoma, and South Dakota explicitly include a provision about personal use of social networking sites. For example, "Employees should be mindful of blurring their personal and professional lives when administering social media, Web 2.0 and social networking sites," Oklahoma's policy warns.

Oklahoma employees are allowed to have their own personal social media presence, so long as it is attached to a personal e-mail and not a state e-mail account. If an employee should decide to comment on official state business through a personal account, that employee is required to state his or her name and role in state government, and include a disclaimer, such as, "This posting on this site are my own and don't reflect or represent the opinions of the State of Oklahoma or the agency for which I work." Those in executive or management positions are asked to use extra caution when posting on their personal social media sites because the nature of the position can indicate the expression of official state policy.

Policy on personal social media use during work hours differs state by state. Some states have policies that allow for brief access to personal social media sites as long as it does not interfere with that employee's ability to complete his or her work. In North Carolina, for example, the state policy reads: "During normal business hours, employees may use personal social networking for limited family or personal communications so long as those communications do not interfere with their work."

Gant views things a bit differently. "When you're on official business, that's all you can do," he says. This means that logging onto Facebook or Twitter during working hours is reserved for those given the privilege of officially representing the Secretary of State's office -- and these employees are expected to complete their official business quickly. "Accessing social media for personal interests has nothing to do with an employee's job duties for the Secretary of State's office, and such utilization during working hours is not permitted," the policy states.

The policies in place now are definitely not the last word on social media standards. There is recognition that the policies and guidelines are often living documents that will change as the platforms evolve and new challenges arise. According to Gant, "My goal was that this was our first publishing of the policy and we're probably going to go through a number of revisions with things that are good and bad and just update those and keep moving forward."

6/23/10 Version

Social Media and Public Agencies: Legal Issues to Be Aware of

Introduction

However one describes it--social media, Web 2.0 or "the Groundswell"—communication has been transformed by Internet technologies that allow users to communicate directly with each other. A key consequence of this is that traditional institutions (for example, the mainstream media, corporations and public agencies) no longer play a controlling role in information flows.

This shift in the balance of power is illustrated by such phenomena as the viral "United Breaks Guitars" video on YouTube. Millions viewed with the airline traveler's consumer complaint delivered by song. The post resonated with every consumer that identified with the frustration of not having companies take responsibility for their actions.

Another consequence of Web 2.0 is that conversations are occurring in different places and among different people. No longer is the concept of a "community" something that is defined by location.[1]

What Is Social Media?

The terms "social media and "Web 2.0" refer to various activities that integrate technology, social interaction, and content creation. Social media allow people to create web content, organize content, edit or comment on content, combine content, and share content. Social media and Web 2.0 use uses many technologies and forms, including RSS and other syndicated web feeds, blogs, wikis, photo–sharing, video–sharing, podcasts, social networking, social bookmarking, mashups, widgets, virtual worlds, micro–blogs, and more.

Example of social media websites include Twitter, Facebook**,** Digg**,** StumbleUpon**,** Yahoo Buzz**,** Reddit**,** LinkedIn and YouTube. Facebook and LinkedIn help connect friends and colleagues. Digg and Yahoo Buzz promote online articles sharing. YouTube focuses on sharing videos.

Source:
http://www.usa.gov/webcontent/technology/other_tech.shtml

There are a number of implications—both positive and negative--for public officials. The legal issues represent one such set of implications. Issues to be aware of include:

1) First Amendment issues relating to government restrictions on speech,

2) Use of public resource issues,

3) Employee use of social media, both on behalf of the agency and personally,

4) Other employment-related social media issues,

5) Open meeting law issues, and

6) Public records retention and disclosure issues, and

7) Procurement, gift and contract issues, and

8) Equal access/Section 508 (disability access) issues.

In some cases, the task for agency attorneys is to determine what the law requires in a given situation. When that is the case, this paper identifies the law that exists on the point and how some agencies have approached the issue. In other cases, the task is to assess the agency's practices against local requirements. In such instances, this paper merely endeavors to flag the issue as one that needs to be analyzed.

First Amendment Issues

Public Forum Issues for Blogs, Facebook and Interactive Sites

One motivation for public agencies to use social media is that they can be effective mechanisms for sharing important information. However, part of their popularity lies in their interactive capabilities: indeed, the ability to get feedback and energize online communities is one of the emerging powers of Web 2.0 applications.[2]

Thus, while a public agency can control what its part of the conversation says, there are limited options for managing what others might say. Moreover, trying to so do may risk litigation under the civil rights laws.[3]

The degree to which public agencies can control what gets posted on a website, blog or social media site turns on what courts call a "public forum" analysis. The first question is what kind of public forum has a public agency created? There are three possible answers:

1) A traditional public forum,

2) A designated public forum, and

3) A nonpublic forum.[4]

"Traditional public forums" are places like streets, sidewalks, and parks which have been by

tradition or public agency action been devoted to assembly and debate. A nonpublic forum is a place that is not by tradition or designation a forum for members of the public to communicate with each other.[5]

A "designated public forum" involves a situation in which a public agency intentionally opens a nonpublic forum for public discourse. There is a subcategory of a designated public forum that is called a "limited public forum" that refers to a type of nonpublic forum that the public agencies have intentionally opened to certain groups or to certain topics.[6] Public agency meetings are considered limited public forums; the courts have upheld rules of decorum when necessary to prevent a speaker from disrupting a meeting in a way that prevents or impedes the accomplishment of the meeting's purpose.[7]

A threshold issue is whether a public agency has opened its website or other communications vehicle to others to post materials of their choosing. If not, then the website is not a public forum and the agency does not violate First Amendment rights when it excludes content.[8]

If a public agency does allow others to post materials of their choosing on a website, blog or social network site, then a credible argument can be made that the agency has created a designated public forum. This would mean that the agency cannot exclude (or delete) material based on its content unless that restriction served a compelling state interest that is narrowly tailored to achieving that interest.[9] Even if the agency created only a "limited public forum" for certain groups or to certain topics, it cannot delete posts simply because they are critical of the agency, its officials or employees or the agency otherwise dislikes what the posts say.

Dos and Don'ts

Do address first things first: evaluate your agency's website to make sure it is well organized and includes a range of information that the public needs to understand how its government functions, where to get needed information and how to participate in decision-making processes. What Web 2.0 functions might the agency add to its existing website (for example, RSS feeds) that might expand its functionality?

Do consider where blogs, Facebook pages, Twitter and other social media fit in with the agency's overall communications and public engagement strategy. If you do decide to incorporate these, be intentional about the role they play in your strategy and realistic about the time they take to use effectively. Consider adopting a policy that guides staff on the agency's use (for examples, see www.ca-ilg.org/cgitechology).

Do make sure that terms of use and privacy policies in an agency's site encompass social media sites if the agency decides to use them.

Do understand that agency-sponsored blogs and Facebook pages are subject to First Amendment limitations on content-based restrictions on speech; this means that the agency must allow posts that are critical of the agency, misinformed, or otherwise may cause heartburn to agency officials.

Do encourage civility in digital discourse, but understand that there are limits on the extent to which such policies can be enforced.

Strategies to Minimize First Amendment Missteps

Social media site settings are another opportunity to minimize missteps. On Facebook, for example, a public agency has choices on how to set its page up. On a "fan page," an agency may select settings so that only authorized staff can start a new topic. This helps limit topics to ones that are related to agency business.

There is, however, no way to turn off "comments" on a Facebook wall page - even if one restricts the other settings. An excerpt from FAQs on the Facebook-for-Government[10] page explains:

> **How do I turn off comments on posted items?**
>
> You cannot turn off comments on posted items. Facebook's value to you as a politician or government official is in allowing your fans to interact with your content. When people comment on or like your content, it is more likely to be seen by their friends in the newsfeed.
>
> **What control do I have over comments posted on my page?**
>
> You can delete any comment on a page, remove a fan, and can permanently ban a fan from the page if you feel that is necessary.

Although factually and technically a public agency could take these actions to "control" comments posted, the question is under what circumstances it would be lawful to do so.

A potential example is deleting comments because they contain profanity. The United States Supreme Court has recognized that some forms of profanity are protected speech.[11] Even though a public agency might properly ban profanity on certain communications media (as happened in the case involving George Carlin's words that can't be used on the radio),[12] the court has also concluded that the Internet is different than television or the radio.[13]

Note that there's a petition on Facebook asking it to filter profanity[14] but the terms of use do not seem to specifically prohibit profanity. They do prohibit "content that is "hateful, threatening, pornographic, or that contains nudity or graphic or gratuitous violence." Also prohibited is bullying, intimidating or harassing any user.[15]

Do's and Don'ts

Do adopt and publicize a social media policy that limits the purpose of the site to serve as a mechanism for communication between the agency and the public.

Do define what kinds of content fall outside that purpose (including commercial, campaign, discriminatory or profane postings) and include a warning that content outside the purpose are subject to removal.

Do advise staff that they may not delete postings simply because they may be critical of the agency or agency officials.

Given the limitations on how a social media page can be set up, it's important to consider other strategies. One is to adopt a social medial policy. Such policies, among other things, provide an

opportunity to define and limit the scope of its own and others' activities as they relate to the agency's social media site. For example, the City of Seattle's *social media* policy says:

> 8. Users and visitors to social media sites shall be notified that the intended purpose of the site is to serve as a mechanism for communication between City departments and members of the public. City of Seattle social media site articles and comments containing any of the following forms of content shall not be allowed:
>
>   a. Comments not topically related to the particular social medium article being commented upon;
>   b. Comments in support of or opposition to political campaigns or ballot measures;
>   c. Profane language or content;
>   d. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation;
>   e. Sexual content or links to sexual content;
>   f. Solicitations of commerce;
>   g. Conduct or encouragement of illegal activity;
>   h. Information that may tend to compromise the safety or security of the public or public systems; or
>   i. Content that violates a legal ownership interest of any other party.
>
>   These guidelines must be displayed to users or made available by hyperlink. Any content removed based on these guidelines must be retained, including the time, date and identity of the poster when available (see the City of Seattle Twitter, Facebook and CityLink standards).[16]

The policy reserves the city's right to restrict or remove any content that is deemed in violation of its policy or any applicable law; it also indicates its goal of approaching the use of social media tools as consistently as possible, enterprise wide. [17]

Seattle also has a specific *Facebook* policy.[18] That policy requires its staff to post the following warning on its pages:

> Comments posted to this page will be monitored. Under the City of Seattle blogging policy, the City reserves the right to remove inappropriate comments including those that have obscene language or sexual content, threaten or defame any person or organization, violate the legal ownership interest of another party, support or oppose political candidates or ballot propositions, promote illegal activity, promote commercial services or products or are not topically related to the particular posting.

The State of Utah's social media policy[19] gives the following direction to its staff:

Moderating Comments

In some social media formats such as Facebook, Blogs, Twitter responses, etc., you may encounter comments which cause you concern as a moderator or responsible party. If user content is positive or negative and in context to the conversation, then the content should be allowed to remain, regardless of whether it is favorable or unfavorable to the State. If the content is ugly, offensive, denigrating and completely out of context, then the content should be rejected and removed.

Note the use of the word "and" instead of "or" in the last sentence. The content has to be ugly, offensive, denigrating AND completely out of context in order to be rejected.

Bottom Line

In short, if an agency participates in social media, it's safe to assume that inappropriate posts will occur ("trolls" whose goal it is to disrupt discussions and elicit emotional responses abound on the Internet, just as gadflys seem to flock to public agency public comment periods). The legally conservative response is to not delete such posts. Correct any misinformation in an even-toned manner and let others evaluate the information as presented.

Do's and Don'ts

Do take advantage of social media site options specifically designed for government.

Do address campaign advocacy in the agency's social media policy by prohibiting it and publicizing the prohibition.

Do provide employees responsible for managing the agency's social media activities clear guidelines.

Do periodically remind (through AB 1234 training and other mechanisms) local officials and staff of the prohibitions against personal and political use of public resources.

Use-of-Public-Resources Issues and Social Media

Public officials are aware of the restrictions of using public resources for either personal or political purposes.[20] State law says that elected officials and staff may not use public resources for personal or campaign purposes (or other purposes not authorized by law). [21]

Personal Activities

"Personal purpose" means those activities which are for personal enjoyment, private gain or advantage, or an outside endeavor not related to business. "Personal purpose" does not include the incidental and minimal use of public resources, such as an occasional telephone call.[22]

This section suggests that an occasional personal "tweet" or visit to one's personal Facebook page on agency time might not be a violation of the law. Employees should be reminded,

however, that it's important to keep in mind public perceptions (and the "public" includes one's friends and family). It should never appear public servants are spending their time at work doing anything other than the public's business.

And, of course, YouTube makes it possible for the public to record, post and publicize public servants' actions while on duty on the internet. The admonition "don't do anything you don't want to read about on the front page of the newspaper" needs to be updated to include "Don't do anything you don't want to see posted on YouTube." As part of the public agency's overall social media or ethics training, it may be helpful to remind employees of this new reality.

FPPC Investigates Internet Political Activity

The Fair Political Practices Commission is again looking into issues relating to online political activity. This inquiry follows on an analysis launched in response to legislation creating the Bipartisan California Commission on Internet Political Activity. The commission issued a report in 2003, but also concluded ongoing evaluation of developing trends is necessary.

One such trend is the fact that traditional campaign media like slate mailers, direct mail flyers and advertisements - all of which are currently required by the Political Reform Act to include disclosures of their source and financing - are increasingly replaced by email, tweets, websites and YouTube Videos.

To deal with this phenomenon, the FPPC created a subcommittee to brief the full commission about the current state of the disclosure of the sources and financing of Internet political activity; whether voters are subject to false or misleading information regarding the source and funding of Internet political activities; the need, if any, to enhance and protect political activity on the Internet; and the need, if any, for legislative or regulatory actions. The subcommittee's report is due June 2010.

For more information see http://209.63.210.75/subcommittee/index.php

Political Activities

Campaign activities and agency use of social media also present issues. Social media tends to be a hotbed of political expression. According to the Pew Internet and American Life study,[23] the internet is now equal to newspapers and roughly twice as important as radio as a source of election news and information.

Not surprisingly, political advisers and consultants have noticed this phenomenon. As a result, local agencies should be alert to activities occurring which make it appear that the agency is using public resources for political activities, whether candidate campaigns or ballot measure advocacy.[24]

For example, a potential concern is paid political advertising appearing adjacent to a public agency's Facebook page: page visitors may not necessarily be aware that the public agency doesn't control a social media provider's advertising placements. One step is to investigate whether a given social media provider makes options available that limit adjacent political advertising (for example, Facebook has a "government" page option that reportedly does this).

Just as candidates and others sometimes try to use public comment periods to air their views and positions, one can also imagine scenarios in which candidates for local office might want to post content on the agency's Facebook page wall or

some similar venue. For this reason, Seattle's social media policy prohibits comments in support of or opposition to political campaigns or ballot measures.[25]

The strongest position from which to enforce such a policy is for a public agency not to not post content relating to candidate or ballot measure advocacy on the agency's site (including not becoming a fan of candidate or ballot measure advocacy sites). Of course, the usual restrictions on using public resources for campaign activities also apply when posting content to the agency's website or social media outlets. [26]

Restrictions on Employee Postings and Tweets

Another issue for local agencies to be aware of as they contemplate the world of Web 2.0 is the degree to which employees can speak their minds on the Internet. In a recent Deloitte LLP Survey on Ethics in the Workplace, 74 percent of those responding employees readily agreed that use of social media can harm their employers' reputation.[27]

Employers have adopted a number of policies to guide (or restrict) employees' use of social media. Perhaps the most succinct come from the "Gruntled Employees" (www.gruntledemployees.com) blog:

- **Blogging Policy:** Be professional
- **Twitter Policy:** Be professional, kind, discreet, authentic. Represent us well. Remember that you can't control it once you hit "update."

Public agencies have found it helpful to adopt more extensive policies and guidelines: samples can be found at www.ca-ilg.org/socialmediapolicies.

Do's and Don'ts

Do advise employees that social media activities can form the basis of adverse employment activities (for example, conduct unbecoming an officer).

Do advise employees that the same restrictions on employee activities that occur with respect to traditional communications channels (for example, restrictions against sexual harassment and discrimination) also apply to social media channels.

Don't take adverse employment actions in response to an employee's exercise of protected activity (for example, speech concerning public concern, whistle-blowing, and participating in union activities) via social medial sites (just as an agency shouldn't take adverse action based on the employee's protected expression through other channels.

There is legitimate room for debate on whether additional guidance will help avoid embarrassing posts. The Deloitte study notes that nearly half of the respondents said that their employers' policies don't change their behavior in cyberspace. It may be useful, however, to remind employees that standards for employee conduct (for example, conduct unbecoming a police officer) also apply in cyberspace.

Whether or not policies help, it's important for public employers to keep in mind that public agencies may not restrict their employees' First Amendment rights to comment on matters of public interest."[28] In fashioning the law in this area, courts have endeavored to strike a balance between the interests of employees as citizens and the interests of public agency employers in efficiently providing public services through their employees."[29]

Public agencies find themselves litigating these issues when an employee claims that an agency "retaliated" (typically by firing or adverse employment action) against the employee for the employee's exercise of his or her First Amendment rights.

In evaluating such claims, the courts ask a series of questions.[30] The first and perhaps most important relates to the nature of the topic that the employee spoke (or tweeted) about. The question is whether the employee's speech involved issues of "public concern" relating to matters of political, social or other concern to the community.[31] Analysis of public concern is not an exact science.[32] One test is whether the information shared by an employee helps community members make informed decisions about the operation of their government."[33]

Unlawful conduct by a government employee or illegal activity within a government agency is a matter of public concern."[34] Furthermore, "misuse of public funds, wastefulness, and inefficiency in managing and operating government entities are matters of inherent public concern." [35] Note that the whistleblower protection laws also protect employees who express concern about these kinds of issues.[36]

What are *not* issues of public concern? Individual personnel disputes and grievances that are not relevant to the evaluating public agency performance.[37]

Other Employment-Related Social Media Issues

A number of employers use Internet research and social media to find and screen potential employees. One thing for employers to keep in mind is that information (both positive and negative) posted on social media sites can be misleading or downright false. A good practice is to verify information received through social media to maximize the likelihood that agencies are acting on reliable information when making hiring decisions.

In addition, the same requirements relating to fairness (non-discrimination) and privacy (for example, credit checks), apply to online activities. For example, those engaged in hiring activities should be reminded that adverse employment decisions based on religion, race or sexual orientation are just as unlawful if the information is acquired through social media as through other means.

Another good practice is to be clear on what social media strategies the agency supports as an appropriate and helpful use of public resources on agency time versus what activities are personal in nature. An agency's discussions relating to social media use can be a useful opportunity to remind employees and officials about proscriptions against personal use of public resources, whether such use involves personal internet surfing or personal use of social networking sites.[38]

Open Meeting Laws

For some, the Internet is the ultimate meeting place. Everything is fairly public (the qualifier "fairly" has to be inserted because the extensive use of pseudonyms that make it difficult sometimes to determine who is doing the speaking; see also sidebar on page 14 regarding the digital divide).

Unlawful Meetings Via Technology

That having been said, conversations on the Internet among public officials can constitute an unlawful "meeting" within the meaning of open meeting laws. For example, California's Brown Act prohibits decision-makers from:

> us[ing] a series of communications of any kind, directly or through intermediaries, to discuss, deliberate or take action on any item of business that is within the subject matter jurisdiction of the legislative body.[39]

The Attorney General has opined that this section prohibits officials from using email to develop a collective concurrence as to an action to be taken, even if the emails are posted on the Internet and distributed at the next public meeting of the body.[40] This is consistent with the Brown Act's underlying purpose of requiring that people be able to observe decision-maker deliberations.[41]

Dos and Don'ts

Do consider something like Twitter for periodic, brief updates on issues of interest from the agency.

Do advise members of decision-making bodies that texting, tweeting and other forms of communications on issues within an agency's subject matter jurisdiction can present Brown Act and common law bias issues both before and during meetings.

Do consider how social media and the internet can foster public engagement in the agency's decision-making process.

Don't engage in discussions on issues within an agency's subject matter jurisdiction on fellow elected officials' blogs and Facebook pages.

Electronic Postings of Agendas

Although the Attorney General has opined that posting agendas to electronic kiosks that are accessible 24/7 in lieu of a paper posting,[42] there is no guidance yet on whether solely posting on the Internet is acceptable (which leads one to conclude that it is not). The concern would be that the Internet may not meet the requirement that agendas be posted in a location that is "freely" accessible to members of the public.[43] Thus, while it is good practice to post agendas and supporting materials on one's website, an agency still should post a paper copy.

Online Teleconferencing?

Finally, the only reference in the Brown Act relating to the use of technology to have meetings relates to teleconferencing. For purposes of the Brown Act, "teleconference" means a meeting of a legislative body, the members of which are in different locations, connected by electronic means, through either audio or video or both.[44] Special posting requirements apply[45] and each

teleconference location must be accessible to the public.[46] The public must have the opportunity to address decision-makers at each location.[47]

These requirements can be satisfied using webcams and other technologies allow decision-makers to be connected through either audio or video. However, the usual typewritten mode of communication that predominates on blogs, social media sites and other Web 2.0 vehicles tends not to involve audio or video. Moreover, the communications tend to occur sequentially over time as opposed to simultaneously. Nor do Internet communications typically involve allowing the public to be present with decision-makers at the teleconference location.

Using Technology to Foster Public Engagement

A key purpose of the Brown Act is to foster public participation in the decision-making process.[48] There are ways that Web 2.0 technology can support this goal, including that Brown Act's requirement that the public have an opportunity to address decision-makers prior to an item being decided.[49]

For example, local agencies and individual decision-makers can offer residents the opportunity to weigh in on issues pending decision through web forums and similar mechanisms, in addition to at meetings. Of course, whenever and however public input is solicited, it is important to show that decision-makers received and considered such input when making a decision. As discussed previously, it's also important to understand the First Amendment implications to creating such forums.

Public Records/Disclosure Issues

Another question is whether public agency postings on third-party social media sites are public records for purposes of records retention or records production requirements.

Records Retention

In California, records retention is governed by a separate statute than public records production. Local agencies generally must retain public records for a minimum of two years, although some records may be destroyed sooner.[50] Most local agencies adopt record retention schedules as part of their records management system. The Secretary of State provides local agencies with record management guidelines.[51]

There is no definition of the "public records" subject to state records retention statutes.[52] The California Attorney General says that a "public record" for purposes of records retention laws is "a thing which constitutes an objective lasting indication of a writing, event or other information, which is in the custody of a public officer and is kept either (1) because a law requires it to be kept or (2) because it is necessary or convenient to the discharge of the public officer's duties and was made or retained for the purpose of preserving its informational content for future reference."[53]

Under this definition, local agency officials retain some discretion concerning what agency records must be kept pursuant to state records retention laws. Similarly, the Public Records Act allows for local agency discretion concerning what preliminary drafts, notes or interagency or intra-agency memoranda are retained in the ordinary course of business.[54]

Agency Postings Are Public Records in Florida

In 2009, the Florida Attorney General determined that a city Facebook page falls within Florida's definition of public records which includes all "material" "made or received . . .in connection with the transaction of official business by any agency." The AG concluded that the city therefore needed to include such information in its retention policies.

Another issue the AG addressed is whether the city's Facebook friends' information might become a public record. The AG said it couldn't reach a "categorical" conclusion, but suggested that the city include a warning regarding the application of Florida's public records laws. This is the warning the city uses:

> Disclosure
>
> The City of Coral Springs Facebook Fan page is informational only. Should you require a response from the City or wish to request City services, you must go to coralsprings.org/help
>
> Under Florida law, all content on the City's Facebook page is subject to the public records law, Chapter 119, Florida Statutes. By becoming a fan of the City of Coral Springs and/or posting on the City's wall, your information will be a matter of public record. The City is required to retain this information in accordance with the State of Florida retention schedule. This may include information on your own Facebook page. All comments will be maintained for a minimum of 30 days after a forum has ended.

In the city attorney's analysis of the AG opinion, he noted that there is an ancillary issue whether the city has the technological capability to retain Facebook content. He also noted that, under an AG opinion interpreting Florida law, it may be Facebook that is responsible for retaining the content.

These materials are available at www.ca-ilg.org/socialmediaFloridalaw.

It would seem that California local agencies can make a strong argument that social media site content is not 1) "kept", 2) required to be kept by law, and 3) is not necessary to be kept in discharge of a public official's duties or made/retained for the purposes of preserving content for future reference. Stating as much in their records retention schedules would seem to be sufficient.

On the other hand, if a public agency is using social media for public input (for example, to solicit public input on planning issues), the agency will want to capture the input provided for the administrative record.

Records Production

The second question is whether content posted on third-party social media sites are public records which an agency is obliged to produce in response to a California Public Records Act request.

In some ways, analyzing the status of content a public agency may post on social media sites may seem a bit paradoxical. The key purpose of California's Public Records Act is to provide the public with access to information that enables them to monitor the functioning of the government;[55] a similar purpose may be ascribed to state constitutional requirements that public official and public agency writings be open to public scrutiny.[56] Using social media to share information with the public accomplishes that very purpose, without putting the public to the trouble of making records requests and

asking for copies of requested documents.

Of course, not everyone has access to the Internet and it is conceivable that someone who doesn't would ask a public agency to provide a copy of posted information on third party social media sites. This may not be a big deal if the post still is displayed on the social media site, but what if it has been deleted? Alternatively, what if the agency can see information on agency friends' sites that others cannot; what if the agency receives a request for information on an agency's "friend's" page. What would an agency's legal obligations be in these situations?

Under the Public Records Act, "public records" include "any writing containing information relating to the conduct of the public's business prepared, owned, used or retained by any state or local agency regardless of physical form or characteristics."[57] Records include records in any media, including electronic media, in which public agencies may possess records.[58]

The challenge is that agency posts on social media may not, strictly speaking, be held in the possession of public agencies. For example, although Facebook's terms of use indicate that users "own" their information,[59] the terms of use also explain that postings occur to the Facebook "platform"[60] and that such postings give Facebook a non-exclusive and transferable license to that content.[61] The company also reserves the right to make Facebook inaccessible to someone who violates its terms of use.[62] The company also explains that deleting content occurs in a manner similar to emptying the recycle bin on a computer--removed content may persist in Facebook's backup copies for a reasonable period of time (but will not be available to others).[63]

Do's and Don'ts

Do check out the special page Facebook created to help government users of Facebook..

Do address social media content in one's records retention policies as not a public record to be retained.

Do use privacy settings that allow the public to access information on the agency's page without having to become a fan or friend.

Do think of social media as a way of driving people to the agency's website for substantive information as opposed to a place where important public information is posted.

Do post a caution to those who might want to become friends or fans of an agency page that their information may become a disclosable public record.

Do endeavor to make information made available online also available through alternative channels.

Do harmonize the agency's posture on records production and retention with the agency's posted privacy policies so as not to inadvertently send mixed messages.

Do encourage visitors to social media sites to review the site's privacy policy.

There are a variety of cases that indicate that the status of public records is tied to writings that are maintained or in the possession of public agencies.[64] (Although being in the possession of a public agency does not in and of itself make a writing a public record.[65]) Although postings on social media sites are "prepared," "owned" and "used" by local agencies, they are not arguably retained by the agency (particularly if the agency's retention and/or social media policy exclude them from retention schedules). Note too

that agencies are not required to reconstruct electronic copies of records no longer available to the agency in electronic format.[66]

This makes it unlikely an agency will have to recreate or archive its postings on social media sites. In terms of the agency having to disclose information to which it has access through the equivalent of fans or friending, such information arguably does not relate to the "conduct of the public's business." Moreover, there is a privacy argument that people shouldn't have to consent to disclosure of personal information in order to obtain public agency information (for example, if a site user otherwise only makes certain information accessible to those they select--in Facebook parlance, to "friends").

To be careful, a public agency may want to use a variation on the warning used on the Florida city's page (see sidebar on page 12):

> This *[insert agency name]*'s page is for general public information only. Should you require a response from the agency or wish to request agency services, you must go to *[insert name of agency website, if appropriate]* or call the agency at *[insert telephone number]*.
>
> Please also be aware that, under certain circumstance, content appearing on this page may be subject to California's public records laws and subject to disclosure by the agency if requested. This may include information about you that you make available through your privacy settings on this site on your own pages.

Social media mavens may have a different theory, but it may be wise—both operationally and legally--to set the agency's privacy settings so "everyone" as opposed to "friends" or "friends of friends" can see content the agency posts. This avoids putting people in the position of potentially having to reveal personal information (that they prefer to only reveal to "real" friends) in order to access the agency's content.

Alternatively, one can err on the side of caution and take steps to preserve postings on social media as public records. This is how the City of Seattle's social media policy[67] addresses this issue:

6. City of Seattle social media sites are subject to State of Washington public records laws. Any content maintained in a social media format that is related to City business, including a list of subscribers and posted communication, is a public record. The Department maintaining the site is responsible for responding completely and accurately to any public records request for public records on social media. Content related to City business shall be maintained in an accessible format and so that it can be produced in response to a request (see the City of Seattle Twitter, Facebook and CityLink standards). Wherever possible, such sites shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure. Users shall be notified that public disclosure requests must be directed to the relevant departmental public disclosure officer.

7. Washington state law and relevant City of Seattle records retention schedules apply to social media formats and social media content. Unless otherwise addressed in a specific social media standards document, the Department maintaining a site shall preserve records required to be maintained pursuant to a relevant records retention schedule for the required retention period on a City server in a format that preserves the integrity of the original record and is easily accessible. Appropriate retention formats for specific social media tools are detailed in the City of Seattle Twitter, Facebook and CityLink standards.

Access to Technology in California

A June 2009 study by the Public Policy Institute of California reveals interesting trends:

- 76 percent of Californians have access to the Internet;
- Rural Californians are as likely to use the Internet as urban Californians and almost as likely to have access to high speed Internet;
- Latinos are less likely to use information technology than whites, blacks, and Asian Pacific Islanders;
- Those with disabilities also are less likely to use a computer and the Internet;
- Renters are less likely to have access to the Internet and broadband technology than homeowners; and
- Access also varies by income as well.

See http://www.ppic.org/content/pubs/jtf/JTF_DigitalDivideJTF.pdf also available at www.ca-ilg.org/cgitechnology.

For example, the city's Facebook policy[68] provides for the following archiving practices:

- An electronic copy of page content shall be periodically saved to a City server. Any postings by City staff on the Wall will be duplicated on the department's web site, Twitter and/or City Link blogs, which are archived on City servers.

- Each Facebook page will be set up in conjunction with a City e-mail account, which will be set to receive and archive all user comments and fans joining the page for purposes of records retention. Any postings removed from the site will be retained in the same format.

In addition, keep in mind that not all members of a community have access to the internet or the same quality internet (see sidebar on page 14 on the digital divide). Adopt a practice of endeavoring to make the information one makes available through the internet available through other means. Below is an excerpt, for example, of the federal government's social media policy.[69]

> 1. Requirement: Agencies are required to provide members of the public who do not have internet connectivity with timely and equitable access to information, for example, by providing hard copies of reports and forms. For the most part, using social media technologies as an exclusive channel for information distribution would prevent users without internet access from receiving such information. In addition, some social media services require high speed internet access and high bandwidth to be effectively utilized, which may not be available in rural areas or may be unaffordable. In general, this requirement is no different for social media implementations than it is for other electronic service offerings. Programs must simply make alternative, non-electronic, forms of information dissemination available upon request. Resources: OMB Circular A-130 section 8 (See a5(d)) and Appendix IV

Privacy Policies

The overlay of public records and retention requirements creates interesting issues relating to privacy policies posted on sites. Such policies became mandatory for commercial sites in 2004 after the state enacted the California Online Privacy Protection Act of 2003.[70] That act requires commercial websites and online service providers that collect personal information (as defined, which includes such information as names and email addresses[71]) on California consumers to conspicuously post and comply with a privacy policy. Even though the requirement applies to commercial sites and services,[72] privacy policies have become a standard element of most websites, including public agency websites.

As a result, it seems important to make sure that the agency's privacy policy on its site is consistent with the agency's analysis of and approach to public records retention and production. For purposes of using third party social media applications, another issue for public agencies is alerting the public that the information they are sharing is subject to the social media site's privacy policies (in addition to the public agency's analysis of its obligations under the Public Records Act and the agency's own privacy practices).[73] A good practice is to provide a link to

the site's policy, as well as any information about the public agency's policy.

Procurement, Gift and Contract Issues

Procurement Issues

Most social media sites are offered for free and the agency's process for selecting one kind of social media outlet may or may not involve a comparative analysis of terms or capabilities. Public agencies (particularly larger ones with more complex procurement regulations) will want to make sure that the decision to use any given social media service complies with the agency's rules.

Gift Issues

When the federal government started examining social media issues, there was a concern that accepting free services might run afoul of some agencies' gift rules. In California, the Political Reform Act defines a "gift" as "any payment that confers a personal benefit on the recipient, to the extent that consideration of equal or greater value is not received and includes a rebate or discount in the price of anything of value unless the rebate or discount is made in the regular course of business to members of the public without regard to official status.[74]

The Fair Political Practices Commission's regulations relating to gifts to public agencies[75] tie to this definition of gift. [76]

One would assume that a free service that is not tied to official status would fall outside the Political Reform Act's definition of gifts. However, the regulations interpreting the act define "payment" as including the provision of goods or services to an agency,[77] although the regulation only applies to a payment "that is otherwise a gift to a public official."[78] As long as the agency is accessing social media services that are free or offered at the same rates to everyone, it would seem that such services would not be reportable[79] as a gift to the agency.

Indemnification and Other Terms of Use Issues

Most online sites require users to agree to terms of service that include such provisions as:

1. **Indemnification and Defense.** When a public agency creates an account on a social media site, it typically must agree not to sue the site, nor allow the site to be included in suits against the agency. Many sites also require the account owner to pay the site's legal costs arising from such suits.

2. **Applicable Law and Venue.** Most terms of service also assert that a certain state's laws (usually California, but not necessarily always) apply to the terms of use and that the state's courts will adjudicate disputes.

The terms of service represent a binding contract; public agencies should assure that they have taken the steps necessary to bind the agency to such an agreement.

Some companies are willing to negotiate on the substantive provisions in the terms of use, but they may be hesitant to negotiate separate agreements with dozens of different agencies. For example, the FAQ on the "Facebook and Government" page indicates that "at this time Facebook does not have any special legal agreements for state and local governments."[80]

However, the National Association of State Chief Information Officers (NASCIO) has reportedly been engaged with a couple of the larger social media providers on the terms of service issue. The Public Technology Institute (PTI) has reportedly joined state information officers as the advocate for local governments. The International Municipal Lawyers Association (IMLA), representing city and county attorneys has is reportedly joined with the effort as well.

Equal Access/Section 508 Issues

California and the federal government have each committed to make their electronic and information technology accessible to people with disabilities. [81] The requirement applies to those who receive state funding.

Among other things, this means using code that works with readers and other such devices that makes information available on the internet to those with disabilities. The goal is to make sure that disabled employees and members of the public access to information that is comparable to the access available to others.

Some social sites are automatically accessible because they are primarily text (for example, blogs). Others have taken steps to address this issue (see, for example, Facebook's instructions on accessing its site with screen readers at www.facebook.com/help/page=440). The concern is that some multimedia sites may not provide the opportunity to include transcripts or captioning. The federal government is working on this issue, but local agencies using social media may want to make sure the social media tools they use are Section 508 compliant. In addition, a good practice is to post information on Section 508 compliant sites (such as one's own website), so people with disabilities always have an accessible version of the content, and that the official version of content is located on a government website.

Conclusion

Social media offers a variety of new tools to connect with the public. As with any communications tool, the key is to think about how the tool fits in with an overall strategy and what resources will be needed to use the tool effectively. It is also important to understand what role the law plays in their use so no missteps occur.

Endnotes

[1] See, for example, the first two definitions of the word "community" on Dictionary.com:

> 1. A social group of any size whose members reside in a specific locality, share government, and often have a common cultural and historical heritage.
> 2. A locality inhabited by such a group.

[2] *See, for example,* Charlene Li and Josh Bernoff, *Groundswell: Winning in a World Transformed by Social Technologies* (Harvard Press: 2008).
[3] Typically such suits are brought under 42 USC § 1983, the Civil Rights Act of 1871, which provides individuals a way to seek redress of claimed deprivations of constitutionally protected rights.
[4] *See Perry Educ. Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37, 45 (1983).
[5] *Preminger v. Peake*, 552 F.3d 757, 765 (9th Cir 2008).
[6] *Flint v. Dennison,* 488 F.3d 816, 831 (9th Cir. 2007).
[7] *White v. City of Norwalk*, 900 F.2d 1421, 1425-26 (9th Cir. 1990). *See also Norse v. City of Santa Cruz*, --- F.3d ---, 2009 WL 3582694 (9th Cir. 2009) (upholding presiding official's ejection of a person who was disrupting a public meeting and rejecting First Amendment challenge).
[8] *See Vargas v. City of Salinas,* 46 Cal.4th 1, 37 n. 18 (2009) (finding city had no obligation to provide those with a different point of view access to the city's website), *citing United States v. Am. Library Ass'n, Inc.,* 539 U.S. 194, 204-206 (2003); *Arkansas Educ. TV. v. Forbes,* 523 U.S. 666, 673-677 (1998); *Cornelius v. NAACP Legal Defense & Ed. Fund,* 473 U.S. 788 (1985); *Perry Ed. Assn. v. Perry Local Educators' Assn.,* 460 U.S. 37, 46 (1983); *Clark v. Burleigh,* 4 Cal.4th 474, 482-491 (1992)) *See also Sutliffe v. Epping School Dist.*, --- F.3d ----, 2009 WL 2973115 (1st Cir 2009) (noting that it is possible there may be cases in which a government entity might open its website to private speech in such a way that its decisions on which links to allow on its website would be more aptly analyzed as government regulation of private speech); *Hogan v. Township of Haddon*, 278 Fed.Appx. 98, 101-02 (3d Cir 2008) (rejecting elected official's claim that she had a First Amendment right to publish articles in the town newsletter and to post on the town's website and cable channel because these communications vehicles were local government-owned and sponsored, and as such are not public or limited public forums); *Page v. Lexington County School Dist. One*, 531 F.3d 275, 285-85 (4th Cir. 2008) (rejecting claims that links to other websites did not vitiate school district's retention of complete control over its website or create a limited public forum, but noting that had a linked website somehow transformed the website into a type of "chat room" or "bulletin board" in which private viewers could express opinions or post information, the issue would, of course, be different).
[9] *Perry Educ. Ass'n,* 460 U.S. at 45.
[10] Available at http://www.facebook.com/government#!/government?v=wall (click on "resources" tab).
[11] *Cohen v. California,* 403 U.S. 15 (1971) (finding that a state may not, consistently with the First and Fourteenth Amendments, make the simple public display a single four-letter expletive a criminal offense).
[12] *Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726 (1978) (emphasizing the sometimes captive nature of the audience for broadcast media).
[13] *Reno v. ACLU*, 521 U.S. 844 (1997) (finding that case law provides no basis for qualifying the level of First Amendment scrutiny that should be applied to the Internet).
[14] http://www.facebook.com/group.php?gid=94118905649.
[15] *See* Facebook Terms of Use, Section 3 (Safety), items 6 and 7, available at http://www.facebook.com/terms.php?ref=pf .
[16] Seattle Social Media Policy, Section 8, available at http://www.seattle.gov/pan/SocialMediaPolicy.htm .
[17] Seattle Social Media Policy, Sections 9 and 10, available at http://www.seattle.gov/pan/SocialMediaPolicy.htm .
[18] Available at http://www.seattle.gov/pan/SocialMedia_Facebook.htm .
[19] Available at http://www.utahta.wikispaces.net/file/view/State%20of%20Utah%20Social%20Media%20Guidelines%209.22.09.pdf .

[20] *See Stanson v. Mott*, 17 Cal. 3d 206, 210-11 (referring to expenditure of staff "time and state resources" to promote passage of bond act); *Vargas v. City of Salinas*, 46 Cal. 4th 1, 31-32 (2009). *See also People v. Battin*, 77 Cal. App. 3d 635, 650 (4th Dist. 1978) (county supervisor's diversion of county staff time for improper political purposes constituted criminal misuse of public monies under Penal Code section 424), *cert. denied*, 439 U.S. 862 (1978), *superseded on other grounds by People v. Conner*, 34 Cal. 3d 141 (1983); Cal. Gov't Code § 8314.
[21] Cal. Gov't Code § 8314(a).
[22] Cal. Gov't Code § 8314(b)(1).
[23] Smith, Aaron, The Internet's Role in Campaign 2008 (April 15, 2009), available at http://www.pewinternet.org/Reports/2009/6--The-Internets-Role-in-Campaign-2008.aspx
[24] *See Stanson v. Mott*, 17 Cal. 3d 206, 210-11 (referring to expenditure of staff "time and state resources" to promote passage of bond act); *Vargas v. City of Salinas*, 46 Cal. 4th 1, 31-32 (2009). *See also People v. Battin*, 77 Cal. App. 3d 635, 650 (4th Dist. 1978) (county supervisor's diversion of county staff time for improper political purposes constituted criminal misuse of public monies under Penal Code section 424), *cert. denied*, 439 U.S. 862 (1978), *superseded on other grounds by People v. Conner*, 34 Cal. 3d 141 (1983); Cal. Gov't Code § 8314.
[25] Seattle Social Media Policy, Section 8(b), available at http://www.seattle.gov/pan/SocialMediaPolicy.htm .
[26] *See Vargas v. City of Salinas*, 46 Cal. 4th 1, 31-32 (2009). *Stanson v. Mott*, 17 Cal. 3d 206 (1976). *See also People v. Battin*, 77 Cal. App. 3d 635, 650 (4th Dist. 1978) (county supervisor's diversion of county staff time for improper political purposes constituted criminal misuse of public monies under Penal Code section 424), *cert. denied*, 439 U.S. 862 (1978), *superseded on other grounds by People v. Conner*, 34 Cal. 3d 141 (1983). *But see DiQuisto v. County of Santa Clara*, 181 Cal. App. 4th 236 (2010) (majority found that sending an editorial against a ballot measure via email on one's lunch hour constituted advocacy, but involved a minimal use of public resources—note dissenting opinion disagreeing with majority's minimal-use-of-public-resources conclusion).
[27] http://www.deloitte.com/view/en_US/us/About/Ethics-Independence/article/8aa3cb51ed812210VgnVCM100000ba42f00aRCRD.htm
[28] *Eng v. Cooley,* 552 F.3d 1062, 1070 (9th Cir.2009); *Pickering v. Bd. of Educ.,* 391 U.S. 563, 568(1968).
[29] *Id.*
[30] *See Desrochers v. City of San Bernardino*, 572 F.3d 703, 708-09 (9th Cir. 2009): The questions probe whether

(1) The employee spoke on a matter of public concern;

(2) The employee spoke as a private citizen or public employee;

(3) The employee's protected speech was a substantial or motivating factor in the adverse employment action;

(4) The public agency had an adequate justification for treating the employee differently from other members of the general public; and

(5) The public agency would have taken the adverse employment action even absent the protected speech.

The first two prongs of this inquiry address whether the speech should be protected under the First Amendment, while the last three address whether that protected speech caused some retaliatory response. *Huppert v. City of Pittsburg*, 574 F.3d 696, 703 (9th Cir. 2009).
[31] *Gibson v. Office of Atty. Gen., State of Cal.,* 561 F.3d 920, 925 (9th Cir. 2009) (quoting *Connick v. Myers,* 461 U.S. 138, 146 (1983)).
[32] *Weeks v. Bayer,* 246 F.3d 1231, 1234 (9th Cir. 2001).
[33] *Desrochers,* 572 F.3d at 710.
[34] *Thomas v. City of Beaverton,* 379 F.3d 802, 809 (9th Cir.2004).
[35] *Johnson v. Multnomah County,* 48 F.3d 420, 425 (9th Cir.1995).
[36] Cal. Gov't Code §§ 8547-8547.12.
[37] *Rosenberger v. Rector and Visitors of University of Virginia*, 515 U.S. 819, 829 (1995).
[38] *See* Cal. Gov't Code § 8314.
[39] Cal. Gov't Code § 54952.2(b).

[40] 84 Ops. Cal. Att'y Gen. 30 (2001) available at http://ag.ca.gov/opinions/pdfs/00-906.pdf. *See also Wood v. Battle Ground School District*, 107 Wash. App. 550 (2001) (email exchange among school board members amounted to illegal meeting under Washington's open meetings law).
[41] *Coalition of Labor, Agriculture and Business v. County of Santa Barbara Board of Supervisors*, 129 Cal. App. 4th 205 (2d Dist. 2005).
[42] 88 Ops. Cal. Att'y Gen . 218 (2005).
[43] Cal. Gov't Code § 54954.2(a)(1).
[44] Cal. Gov't Code § 54953(b)(4).
[45] Cal. Gov't Code § 54953(b)(3) ("If the legislative body of a local agency elects to use teleconferencing, it shall post agendas at all teleconference locations . . . ").
[46] Cal. Gov't Code § 54953(b)(3) ("Each teleconference local shall be identified in the notice and agenda of the meeting or proceeding, and each teleconference location shall be accessible to the public. ").
[47] Cal. Gov't Code § 54953(b)(3) ("The agenda shall provide an opportunity for members of the public to address the legislative body directly pursuant to Section 54954.3 at each teleconference location.")
[48] *Coalition of Labor, Agriculture and Business v. County of Santa Barbara Board of Supervisors*, 129 Cal. App. 4th 205 (2d Dist. 2005).
[49] Cal. Gov't Code § 54954.3(a) ("Every agenda for regular meetings shall provide an opportunity for members of the public to directly address the legislative body on any items of interest to the public, before or during the legislative body's consideration of the item, that is within the subject matter jurisdiction of the legislative body, provided that no action shall be taken on any item not appearing on the agenda . . . ").
[50] Cal. Gov't Code § 34090(d). Note that in California, the Public Records Act is not a records retention statute. *See Los Angeles Police Dept. v. Superior Court,* 65 Cal. App. 3d 661 (1977).
[51] The Secretary of State's Local Government Records Management Guidelines may be viewed at http://www.sos.ca.gov/archives/local-gov-program/pdf/records-management-8.pdf
[52] 64 Cal. Ops.Att'y Gen. 317 (1981).
[53] 64 Cal. Ops. Att'y Gen. 317 (1981).
[54] Cal. Gov't Code § 6254 (a).
[55] *U.S. Dept. of Justice v. Reporters Com. for Freedom of Press,* 489 U.S. 749 (1989); *CBS, Inc. v. Block,* 42 Cal.3d 646 (1986); *Times Mirror Co. v. Superior Court,* 53 Cal. 3d 1325 (1991). Note that California's Public Records Act provides for two types of access. One is a right to inspect public records. *See* Cal. Gov't Code § 6253(a). The other is a right to prompt availability of copies of those records. *See* Cal. Gov't Code § 6253(b).
[56] *See* Cal. Const., art. I, § 3(b)(1) ("The people have the right of access to information concerning the conduct of the people's business, and, therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny.").
[57] Cal. Gov't Code § 6252(e).
[58] The definition of "writings" includes any "transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored." Cal. Gov't Code § 6252(g). Note too that some provisions of the Act deal explicitly with electronic records.
[59] *See* December 21, 2009 Facebook Terms of Use Policy, #2:

> **2. Sharing Your Content and Information**
>
> You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
>
> 1. For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.

2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
3. When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share. (To learn more about Platform, read our About Platform page.)
4. When you publish content or information using the "everyone" setting, it means that everyone, including people off of Facebook, will have access to that information and we may not have control over what they do with it.
5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

[60] *See* Facebook Terms of Use, #17 (Definitions):

17. Definitions

1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; and (c) other media, software (such as a toolbar), devices, or networks now existing or later developed.

2. By "us," "we" and "our" we mean Facebook, Inc., or if you are outside of the United States, Facebook Ireland Limited.

3. By "Platform" we mean a set of APIs and services that enable applications, developers, operators or services, including Connect and RSS feeds, to retrieve data from Facebook or provide data to us.

4. By "information" we mean facts and other information about you, including actions you take.

5. By "content" we mean anything you post on Facebook that would not be included in the definition of "information."

6. By "data" we mean content and information that third parties can retrieve from Facebook or provide to Facebook through Platform.

7. By "post" we mean post on Facebook or otherwise make available to us (such as by using an application).

8. By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.

[61] *See* Facebook Terms of Use, #2(1) (above).
[62] *See* Facebook Terms of Use, #14 (Termination) (" If you violate the letter or spirit of this Statement, or otherwise create possible legal exposure for us, we can stop providing all or part of Facebook to you.")
[63] *See* Facebook Terms of Use, #2(2) (above).
[64] *See Gilbert v. City of San Jose,* 114 Cal.App.4th 606, 610 (6th Dist.2003) (noting the Public Records Act "provides for the inspection of public records *maintained by* state and local agencies" and noting the Records Act's purpose was "to give the public access to information in possession of public agencies . . ."), citing *California State University, Fresno Association, Inc. v. Superior Court*, 90 Cal. App. 4th 810, 822 (5th Dist. 2001), and *CBS, Inc. v.*

Block, 42 Cal.3d 646 (1986). This language is quoted in *BRV, Inc. v. Superior Court***,** 143 Cal. App. 4th 742, 750 (3d Dist., 2006) and *Versaci v. Superior Court***,** 127 Cal. App. 4th 805, 813 (4th Dist.,2005).

[65] *See Braun v. City of Taft,* 154 Cal. App. 3d 332, 340 (1984) ("The mere custody of a writing by a public agency does not make it a public record, but if a record is kept by an officer because it is necessary or convenient to the discharge of his official duty, it is a public record."), also *quoted in California State University v. Superior Court*, 90 Cal. App. 4th at 810.

[66] Cal. Gov't Code § 6253.9(c).

[67] Available at http://www.seattle.gov/pan/SocialMediaPolicy.htm

[68] Available at http://www.seattle.gov/pan/SocialMedia_Facebook.htm .

[69] *See* General Services Administration, Social Media Handbook, Chapter 8, available at http://www.gsa.gov/graphics/staffoffices/socialmediahandbook.pdf

[70] *See* Cal. Bus. & Prof. Code §§ 22575-22579.

[71] Cal. Bus. & Prof. Code § 22577(a). The full definition reads:

> For the purposes of this chapter, the following definitions apply:
>
> (a) The term "personally identifiable information" means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:
>
> (1) A first and last name.
> (2) A home or other physical address, including street name and name of a city or town.
> (3) An e-mail address.
> (4) A telephone number.
> (5) A social security number.
> (6) Any other identifier that permits the physical or online contacting of a specific individual.
> (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

[72] Cal. Bus. & Prof. Code § 22577(a). The full definition reads:

> (c) The term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.
> (d) The term "consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.

[73] For more on the Online Privacy Protection Act and best practice recommendations on online and off-line privacy policies, see our Recommended Practices on California Information-Sharing Disclosures and Privacy Policy Statements, available at www.privacy.ca.gov (specifically at http://www.privacy.ca.gov/res/docs/pdf/infosharingdisclos.pdf).

[74] *See* Cal. Gov't Code § 82028. See also Cal. Gov't Code § 82044 ("'Payment' means a payment, distribution, transfer, loan, advance, deposit, gift or rendering of money, property, services or anything else of value, whether tangible or intangible.")

[75] *See* 2 Cal. Code of Regs. § 18944.2.

[76] *See* 2 Cal. Code of Regs. § 18944.2(c) ("A payment, that is otherwise a gift to a public official, as defined in Section 82028, shall be considered a gift to the public official's agency and not a gift to the public official if all of the following requirements are met . . . ").

[77] *See* 2 Cal. Code of Regs. § 18944.2(b)(1).

[78] *See* 2 Cal. Code of Regs. § 18944.2(c). The full language reads: "A payment, that is otherwise a gift to a public official, as defined in Section 82028, shall be considered a gift to the public official's agency and not a gift to the public official if all the following requirements are met: . . .").
[79] *See* 2 Cal. Code of Regs. § 18944.2(c)(3) (requiring agencies to report gifts received within 30days of receipt).
[80] *See* www.facebook.com/help/?page=440#!/government?v=app_4949752878 (under the "resources" tab, under FAQs).
[81] *See* 29 U.S.C. § 794d (often known as "Section 508" for its number in the Rehabilitation Act). The procurement standards from Section 508 of the Rehabilitation Act are referred to in California Government Code Section 11135-11139.8, which provides protection from discrimination from any program or activity that is conducted, funded directly by, or receives any financial assistance from the state. This section brings into state law the protection of Title II of the ADA which ensures accessibility to government programs and also requires state government to follow accessibility requirements standards of Section 508 of the Rehabilitation Act, which ensures the accessibility of electronic and information technology. For more information on these issues, see http://www.disabilityaccessinfo.ca.gov.

8a

January 12, 2011

TO: Local Agency Formation Commission

FROM: Executive Officer
Assistant Executive Officer

SUBJECT: Proposed Policy for Using Social Media

Background

At the Commission's annual strategic planning session in August 2010, staff was directed to explore the use of social media to enhance communication among LAFCO's stakeholders. Social media tools include (but are not limited to) the Internet, cell phones/Blackberries, Facebook, Twitter, MySpace and LindedIn.

Staff developed a draft Social Media Policy (***Attachment 1***) intended to provide staff and the Commission with guidance on the use of computer and telecommunication equipment and social networking media.

The draft policy was introduced at the Commission's November 10, 2010 meeting. Because of the length of the policy, additional time was provided for the Commission to review the policy and offer comments, if any, prior to staff bringing the policy back for final review and adoption. To date, staff has received no comments from the Commission on the draft policy.

Staff is recommending that the Commission adopt the policy, as drafted, and direct staff to incorporate the policy into the Commission's 2011 Policies and Procedures Handbook.

However, as the use of social media tools is refined over time, the Social Media Policy will require additional review and revisions by the Commission. One opportunity is during the annual Policies and Procedures Handbook update, which offers an opportunity to reevaluate and update all of the Commissions policies and procedures. The next comprehensive Policies and Procedures Handbook update is scheduled for the Commission's February 9, 2011 meeting.

Staff will be monitoring the effectiveness of the two social media tools authorized by this Commission—Facebook and Twitter—over the next year and will recommend changes as needed.

Recommendations

1. Adopt the proposed Social Media Policy (***Attachment 1***).

Respectfully submitted,

JOYCE CROSTHWAITE

CAROLYN EMERY

Attachment 1: Draft Social Media Policy

Attachment 1

Social Media Use Policy

I. Purpose

The purpose of this policy is to provide clear and concise direction regarding the appropriate use of LAFCO's computers, telecommunication equipment, social media tools and software.

II. Policy Statement

The Orange County Local Agency Formation Commission (OCLAFCO) provides computer and telecommunication equipment to both staff and Commissioners for the efficient performance of their duties. OC LAFCO also uses social media sites and tools to maintain effective communication with OC agencies and the public.

This policy applies to all employees, all Commissioners, consultants, interns, volunteers and other non-employees who use OC LAFCO's computers or telecommunication equipment. Each person covered by this policy has a responsibility to use LAFCO's computers, telecommunication equipment, social media tools and software in a manner that enhances LAFCO's public image and increases productivity. Failure to follow this policy may lead to disciplinary measures up to and including termination of employment.

III. Computer and Telecommunications Equipment

LAFCO's computer and telecommunications equipment consists of all electronic devices, software, and means of electronic communication including, but not limited to, the following equipment: personal computers and workstations; iPads; notebooks, laptops, and other mobile computers; mini and mainframe computers; computer hardware such as flash drives, disk drives and tape drives; peripheral equipment such as printers, modems, fax machines, video recorders, digital cameras, projectors and copiers; computer software applications and associated files and data, including software that enables access to external services, such as the Internet/Intranet; electronic mail (e-mail); telephones; cellular phones; pagers; and voicemail systems (equipment).

- **Access to computer and telecommunications equipment, messages, and electronic data**

  Access to LAFCO's computer and telecommunications equipment is within the sole and exclusive discretion of LAFCO. The Executive Officer can authorize access of LAFCO's computer and telecommunications equipment subject to the user's written agreement to comply with this policy. All messages sent and received, including personal messages, and all data and information stored on LAFCO's electronic-mail system, voicemail system, or computer systems are LAFCO property regardless of the content, including occasional personal voicemail and e-mail. LAFCO reserves the right to access all of its computer and telecommunications equipment at any time, at its sole and exclusive discretion, without prior notice to the user.

LAFCO personnel have no right of privacy with respect to any messages or information created or maintained on LAFCOs computer and telecommunications equipment. LAFCO may, at its discretion, inspect all files or messages on its computer and telecommunications equipment at any time for any reason. LAFCO, at its sole and exclusive discretion also may monitor its computer and telecommunications equipment at any time, without prior notice to the user, in order to determine compliance with LAFCO policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

LAFCO personnel should understand that any information kept or sent on LAFCO's computer and telecommunications equipment may be electronically recalled or recreated regardless of whether it may have been deleted or erased by a user. LAFCO assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on LAFCO's computer and telecommunications equipment. LAFCO accepts no responsibility or liability for the loss or non-delivery of any personal e-mail or voicemail communications or any personal data stored on any LAFCO property. LAFCO strongly discourages storage of any important or sensitive personal data, on any of LAFCO's computer and telecommunications equipment.

- **Proper use of LAFCO's computer and telecommunication equipment**

  LAFCO's computer and telecommunications equipment is to be used by LAFCO personnel only for the purpose of conducting LAFCO business and LAFCO-approved activities, including communication with citizens, member agencies, contractors and LAFCO service providers; legal and factual research; and other similar activities, except as otherwise provided.

  LAFCO personnel may use LAFCO's computer and telecommunications equipment for the following incidental personal uses as long as it does not interfere with the user's duties, does not conflict with the LAFCO's business, is at no cost to LAFCO and does not violate either this or any other LAFCO policy:

  1. To send and receive occasional personal e-mail and other communications;

  2. To prepare and store incidental personal data (such as personal calendars, personal address lists, and similar incidental personal data) in a reasonable manner;

  3. To use the telephone system for brief and necessary personal calls,

     at the caller's expense for toll calls; and

  4. To access the Internet for brief personal searches and inquiries outside of established work hours, provided that user complies with all other LAFCO policies.

- **Improper use of LAFCO's computer and telecommunications equipment**

    1. Prohibition Against Harassing, Discriminatory and Defamatory Use

       Under no circumstances may LAFCO personnel use LAFCO's computer and telecommunications equipment to transmit, receive, or store any information that is discriminatory, harassing, or defamatory in any way (e.g., sexually explicit or racist messages, jokes, or cartoons). Any use of LAFCO computers or telecommunication equipment for the transmission or storage of pornography shall be immediately reported to appropriate legal authorities.

    2. Prohibition Against Violating Copyright Law

       LAFCO personnel must not use LAFCO's computer and telecommunications equipment to copy, retrieve, forward or send copyrighted materials unless the user has LAFCO's and the author's permission or is accessing a single copy only for the user's reference for LAFCO-related work.

    3. Other Prohibited Uses

       Under no circumstances may LAFCO personnel use LAFCO's computer and telecommunications equipment for any illegal purpose, to disclose confidential or proprietary information of LAFCO or third parties, to conduct non-LAFCO business, to solicit or proselytize others for commercial ventures, religious or political causes, or for other purposes not related to the user's duties or responsibilities to LAFCO, except for incidental personal use, as provided in the previous section.

- **Cellular Phones**

  The issuance of LAFCO-owned cellular phones is subject to approval by the Executive Officer. When possible and practical, desk phones should be utilized prior to the use of cellular phones.

- **The Internet and On-Line Services**

  LAFCO provides access to the Internet and on-line service providers. LAFCO expects that all users will use these services in a responsible manner and for LAFCO-related business purposes only, except as otherwise provided in previous sections. These LAFCO-related purposes include legal and factual research, electronic communication and transmission of information.

  LAFCO personnel shall not use LAFCO's computer and telecommunications equipment to access, download posts or contribute to sites displaying:

    1. Gross, indecent, obscene, harassing, pornographic or sexually explicit materials;

    2. Gambling;

3. Illicit drugs;

4. Illegal activity.

LAFCO personnel shall not sign guest books at websites or post messages to Internet news groups, website discussion groups, or social networking web sites except for LAFCO-related business.

IV. Social Networking

The Executive Officer shall maintain a list of social media tools, as approved by the Commission, which are approved for use by LAFCO staff. The Executive Officer or designee will also maintain a list of LAFCO's login and password information. The Executive Officer or designee will inform the Commission of any new social media sites or administrative changes to existing sites. LAFCO must be able to immediately edit or remove content from social media sites.

LAFCO's website (http://www.oclafco.org) will remain LAFCO's primary and predominant internet presence. The most appropriate uses of social media tools increase LAFCO's ability to reach the widest possible audience. Wherever possible, content posted to LAFCO's social media sites will also be made available on the LAFCO website. The Executive Officer or designee will be responsible for the content and upkeep (including maintenance and monitoring) of all LAFCO social media sites.

The following social media tools have been approved by the LAFCO Commission and standards have been developed for their use:

1. Twitter
2. Facebook
3. Video Posts

The use of other sites must be approved by the LAFCO Commission.

LAFCO's social media sites shall comply with all appropriate LAFCO policies and procedures and are subject to the California Public Records Act and Proposition 59 (Open Meeting Laws and Public Disclosure), amending Article 1, Section 3 of the California Constitution. Any content maintained in a social media format that is related to LAFCO business, including a list of subscribers and posted communication (with certain exceptions), is a public record. Content related to LAFCO business shall be maintained in an accessible format and so that it can be produced in response to a public records request. The Executive Officer is responsible for responding completely and accurately to any public records request for public records on social media.

Users and visitors to LAFCO's social media sites shall be notified that the intended purpose of the site is to serve as a means of communication for LAFCO. LAFCO's social media site articles, posts and comments shall conform to all of LAFCO's content policies. Users shall be informed by posting to the LAFCO's social media sites that LAFCO disclaims any and all responsibility and liability for any materials that LAFCO deems inappropriate for posting, which cannot be removed in an expeditious and otherwise timely manner.

These guidelines must be displayed to users or made available by hyperlink. Any

content removed based on these guidelines must be retained, including the time, date and identity of the poster when available (see LAFCO's Facebook and Video Posting standards), in accordance with LAFCO's policy on the retention of such information. LAFCO reserves the right to restrict or remove any content that is deemed in violation of this policy or any applicable law.

Twitter Standards

Twitter is micro-blogging tool that allows holders to tweet up to 140 characters of information to followers. By procuring and maintaining Twitter accounts, LAFCO will communicate information directly to their Twitter followers, alerting them to news and directing them to the LAFCO's website for more information.

- Purpose

  Twitter accounts shall serve three primary purposes:

  1. Disseminate immediate, interesting and important information;
  2. Promote LAFCO-sponsored meetings, events and programs;
  3. Refer followers to a news item or content hosted on LAFCO's website.

- Content

  The Executive Officer or designee shall hold and maintain LAFCO's Twitter account. LAFCO will have only one Twitter account. Account information, including usernames and passwords, shall be kept by the Executive Officer.

  LAFCO's biography and/or background information will include a link to LAFCO's website where the following disclaimer information will be posted:

  > "This is an official Orange County LAFCO Twitter account. For more information about LAFCO, please visit www.oclafco.org. This site is intended to serve as a mechanism for communication between the public and LAFCO on LAFCO-related topics and as a forum to further the mission of LAFCO. Any direct tweets to this page and its list of followers may be considered a public record which is subject to disclosure pursuant to the California Public Records Act. Public information requests must be directed to the Executive Officer."

  LAFCO's Twitter username shall begin with "OCLAFCO". The main image shall be LAFCO's logo. Information posted on Twitter shall conform to the existing policies of LAFCO. Tweets shall be relevant, timely and informative. Twitter content, as much as possible, shall mirror information presented on the LAFCO website. The Executive Officer or designee shall ensure that information is posted correctly the first time. LAFCO will use proper grammar and standard AP style, and will avoid the use of jargon and abbreviations. Twitter is more casual than most other communication tools, but communications must still reflect the professionalism of LAFCO at all times.

Facebook Standards

Facebook is a social networking site that continues to grow in popularity and functionality. Businesses and government agencies have joined individuals in using Facebook to promote activities, programs, projects and events. These standards are designed for LAFCO to drive traffic to its website and to inform more people about LAFCO activities. As Facebook changes, these standards may be updated as needed.

- Establishing a Page

  Applications will not to be added to the LAFCO's Facebook site without the express written approval of the Executive Officer. The Executive Officer or designee will register the page with a LAFCO email address. Personal Facebook profiles shall not be used to administrate LAFCO pages.

- Type of "Pages"

  LAFCO will create "pages" in Facebook (not "groups"). Facebook "pages" offer distinct advantages including greater visibility, customization and measurability.

- Format

  For 'type' description, choose "government." The main image shall be LAFCO's logo or an appropriate photo. LAFCO will include the agency's mission statement in the introduction box on the Wall Page. Using the FBML static page application, a boilerplate section should contain a description of LAFCO and the following:

  > "This is an official Facebook page of LAFCO of Orange County. For more information about LAFCO please visit www.oclafco.org. This site is intended to serve as a mechanism for communication between the public and LAFCO on the listed topics and as a forum to further the mission of LAFCO. Any comment submitted to this page and its list of fans may be considered a public record which is subject to disclosure pursuant to the California Public Records Act. Public information requests must be directed to the Executive Officer."

  If comments are turned on, the FBML page shall also include a Comment Policy Box with the following disclaimer:

  > "Comments posted to this page will be monitored and inappropriate content will be removed as soon as possible. Under LAFCO Social Media Use Policy, Standards and Procedures, LAFCO reserves the right to remove inappropriate content, including, but not limited to, those items that have obscene language or sexual content, threaten or defame any person or organization, violate the legal ownership interest of another party, promote illegal activity and promote commercial services or products. LAFCO disclaims any and all responsibility and liability for any materials that LAFCO deems inappropriate for posting, which cannot

be removed in an expeditious and otherwise timely manner."

- Page Administrators

  The Executive Officer will designate one or more staff members as page administrators who will be responsible for monitoring LAFCO's Facebook page. Only designated LAFCO staff members will make posts. The Executive Officer or designee will be responsible for ensuring content is not stale.

- Comments and Discussion Boards

  Comments to the Wall Page will be monitored once a week. If LAFCO is unable to monitor content weekly, comments to the Wall shall be turned off. Discussion Boards shall be turned off unless specifically approved by the Commission.

- Photos and Video

  Page administrators may add photos and videos to LAFCO's Facebook page. If there are postings of photos and/or videos of the public, staff must secure waivers by individuals depicted in the photo and/or video. Photos and/or videos of LAFCO's employees taken during regular office hours may be posted without obtaining waivers. Videos must follow the Video Posting Standard. The ability for fans to post photos, videos and links shall be turned off.

- Applications

  Common Facebook applications can allow users to stream video and music, post photos, and view and subscribe to RSS feeds. An application must not be used unless it serves an appropriate and a valid business purpose, adds to the user experience, comes from a trusted source, and is approved by the Executive Officer. An application may be removed at any time if LAFCO determines that it is causing a security breach or spreading viruses.

- Archive

  The Executive Officer or designee will maintain an electronic record or printout of any information necessary to retain for the purposes of public records retention in accordance with the applicable LAFCO policy regarding retention of such information.

- Indemnity

  LAFCO shall take all necessary steps to bind the agency to all required terms of service prior to establishing a Facebook account.

Video Posting Standards

LAFCO will enable access to online video content to enhance the public's ability to access LAFCO-related information online. Key objectives for video content shall meet one or more of the follow goals:

1. To further LAFCO's mission;
2. To provide information about LAFCO services; and,
3. To showcase LAFCO, community events and explore LAFCO issues.

LAFCO encourages the use of video content to further the goals of the LAFCO where appropriate. These standards should be used in conjunction with the LAFCO's Social Media Use Policy, Standards and Procedures:

- Video Posting Guidelines

  The Executive Officer or designee will be responsible for approving the video content. Video quality must be comparable to DVD resolution quality. Low quality video will be considered as long as the audio portion is clear and the content is compelling and informative. All videos must be posted on LAFCO's website and the department's Facebook page. LAFCO must secure a disclaimer from the author or owner or the right to use all of or part of a video if the video was not produced by LAFCO.

  Videos streamed from other sources may not be posted to LAFCO's website without written permission of the Executive Officer. Links to external videos are permitted, but it must only be used when content is relevant and written approval of the Executive Officer is received.

- Submitting Videos to Hosting Sites

- Videos may be submitted to hosting sites such as YouTube and Vimeo as well as Facebook on a case-by-case basis under the direction of the Executive Officer or designee. Most of these sites limit the video to the lesser of 10 minutes in length or less than 1 GB of data storage. Comments posted to these sites must be monitored or the ability to post a comment shall be turned off. Comments must adhere to the guidelines stated in this policy.

- Archive

  Any video posted to a third party's video site must also be posted to LAFCO's website for purposes of records retention.

V. SOFTWARE USE ON LAFCO's COMPUTER AND TELECOMMUNICATIONS EQUIPMENT

No software is to be installed, downloaded or used on LAFCO's computer and telecommunications equipment that has not been paid for and appropriately licensed. No user may load any software on LAFCO's computers, by any means, unless authorized in writing in advance by the Executive Officer or designee. Authorization to load software onto LAFCO's computers will not be given until the software to be loaded has been scanned thoroughly for viruses.

- **LAFCO Software for Home Use**

  Use of software purchased by LAFCO on home computers is generally prohibited but may be allowed in certain situations based on the licensing provisions of the software. Before installing, transferring, or copying any software from media or directly from LAFCO's computer and

telecommunications equipment to another computer, LAFCO personnel must request permission and receive written authorization from the Executive Officer or designee.

VI. CONFIDENTIAL INFORMATION AND SECURITY ISSUES

LAFCO must be sensitive to the protection of privileged communications, trade secrets and other confidential and proprietary information of both LAFCO and third parties (Confidential Information). Therefore, LAFCO personnel are expected to use reasonable judgment and to adhere to the highest ethical standards when using or transmitting Confidential Information on LAFCO's computer and telecommunications equipment. Confidential Information shall not be accessed through LAFCO's computer and telecommunications equipment in the presence of, or transmitted to, unauthorized individuals. Similarly, confidential Information should not be left visible on a computer screen, nor should a computer screen showing confidential information be left unattended.

LAFCO's computer and telecommunications equipment can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. LAFCO personnel are expected to maintain the confidentiality of their passwords. LAFCO personnel should use care in the creation of passwords and should not use passwords that might be readily deduced by unauthorized users.