

By considering each of these eight essential elements, governments can largely address many of the current concerns surrounding social media use:

1. Employee Access

Governments have discretion, through Web site filtering tools, to restrict access to areas of the Internet deemed non-work related, such as personal email or leisure Web sites. Up until the last two years, social media sites have tended to fall under the non-work related umbrella. However, increasingly social media sites are blurring the line between personal, professional, and official agency use, raising new questions of which employees may access social media sites and what should be the process for gaining access.

Government agencies are managing access in two ways: 1) by controlling the number or types of employees who are allowed access to social media sites or 2) by limiting the types of sites that are approved for employee access. Most of the agencies we interviewed limited employee access to social media, allowing access for only a handful of designated individuals or functions (e.g., leadership or public information officers). Only one of the interviewed agencies allowed all employees unrestricted access to all social media sites.

Other agencies managed access by allowing all employees access to pre-approved social media sites. According to one interviewee, "Our agency allowed viewing access to YouTube after a risk assessment determined there is a business need for it and that the benefits outweighed the risks. All other sites are being blocked. If there is a need or request, it will be evaluated on a case by case basis by the director."

In agencies with formal policies, some outline required procedures for gaining access to social media sites. Of the 26 policies and guidelines reviewed, five addressed procedures for access. Of those five, most required employees or departments to submit an official business case justification in order to access and use social media sites.

Based on our interviews, the balance between unrestricted and controlled access remains a dilemma for many agencies. While some agencies may value the potential opportunities for professional development when employees are engaged in educational, collaborative, or knowledge sharing activities fostered by open access to social media sites, many still are fearful of the perceived legal and security risks. In addition, once access policy is determined, questions of account management and acceptable use inevitably arise.

Sample language for requesting access

"All social media requests must be submitted in the form of a business case to the Deputy County Executive for Information, who will then consult with the E-Government Steering Committee. If approved, agencies must fill out and have an agency director sign the Procedural Memorandum 70-05 Revised: Request for Waiver/Exemption Form and return it to the Information Security Office in the Department of Information Technology"

~Fairfax County, VA

2. Social Media Account Management

Account management encompasses the creation, maintenance, and destruction of social media accounts. Establishing an account on a social media site provides an employee with the full range of tools and capabilities for that site, such as joining networks or posting information. The lack of a clearly defined policy on account management may result in a situation where agency leadership does not have a handle on what types of social media accounts are being established, maintained, or closed by their employees for professional or official agency use. Therefore, a critical element to a social media policy for many is establishing who may set up an agency or professional social media account, as well as a procedure for establishing an account.

In the policies reviewed, the strategies varied. One strategy was to require approval by only one designated party, which was most frequently the public information officer. The State of North Carolina outlined who is responsible for approving and maintaining accounts and what happens when accounts are removed. Other strategies involve approval by more than one party. For example, Arlington County, Virginia requires approval from both the communication department and the IT department.

While our sample of government policies is too small to draw any definite conclusions, local government policies tend to be more explicit on account management as compared to state or federal agencies. Twelve of the policies and guidelines reviewed addressed the element of account management, and eight of those 12 came from local

government. One reason for this difference might be scale and the level at which issues are addressed within policies. In comparison, state policies tended to provide enterprise level suggestions and thus steered away from specific management issues.

Sample language outlining multiple approvals needed to create a social media account

"There should be an authorization process for employees wishing to create an account for the benefit of the agency, with the agency Public Information Officer (PIO) as the authority to oversee and confirm decisions. In this role, the PIO will evaluate all requests for usage, verify staff being authorized to use social media tools, and confirm completion of online training for social media.

PIOs will also be responsible for maintaining a list of all social networking application domain names in use, the names of all employee administrators of these accounts, as well as, the associated user identifications and passwords currently active within their respective agencies."

~State of North Carolina

3. Acceptable Use

Acceptable use policies typically outline an organization's position on how employees are expected to use agency resources, restrictions on use for personal interests, and consequences for violating the policy.

Twelve of the policies and guidelines we reviewed deal specifically with acceptable use, particularly for personal interests. The majority of these 12 policies point toward existing policies that already dictate acceptable use of common electronic and information resources such as telephone, computer, or Internet access.

However, as the use of social media in government evolves over time, acceptable use policies may need to address the blurring boundaries around personal, professional, and official agency use. In our interviews, we found that agencies are struggling with what is acceptable in terms of employees' personal and professional use of social media. Questions commonly arise with social media use, such as how much time an employee may spend on a personal Facebook page while at work or how much time an employee should devote to participating in peer-to-peer networking on sites such as GovLoop.

Unlike the question of acceptable personal use during designated times or non work hours, the question of acceptable employee use for professional and official agency reasons remains complicated. Only three of the 26 policies have begun to address this issue.

Some government agencies draw a clear distinction between an employee's professional use of social media and an employee's personal use of the same tools. For example, in the City of Arvada, Colorado, the social media policy clearly states, "Social Media use is for business communication and for the purpose of fulfilling job duties, in accordance with corporate goals and objectives, not for personal use." On the other hand, the US Air Force encourages its members to think of themselves as on duty 24 hours a day, seven days a week when it comes to social media use. Others we interviewed suggested acceptable employee use for professional interest is better monitored and managed by supervisors, rather than a one-size fits all policy.

Sample language for addressing acceptable use of social media sites for personal use while at work.

"Employees should follow regulations and policies according to the City's Email and Electronic Communication Acceptable Use Policy. Some aspects of that policy that relates to employees' use of social media/networking resources include the following:

1. . . .
2. Use of the City-provided Internet Email and Lotus Notes is a privilege. Unauthorized use will result in the loss of access for the user and, depending on the seriousness of the infraction, may result in disciplinary action as deemed appropriate.
3. Employees should recognize that there are restrictions and limitations to use of the Internet and its related technologies. There is a limited amount of personal use that is understood and permissible, but employees should be as conservative as possible in such personal use and understand that public records laws may bring their use under scrutiny by the media and public."

~City of Chandler, AZ

4. Employee Conduct

In general, professional employee conduct is already governed by policies such as an ethical code of conduct that addresses what is “right” and “wrong” in terms of employees’ behavior, and sets out the consequences should a violation occur. Twenty-one of the reviewed policies addressed employee conduct in their professional capacity, with the majority of them referencing existing policies by either using direct quotes or simply providing links or reference numbers on where to look further.

In addition to a standard conduct code that addresses things such as racially offensive language, some of the policies do address issues more specific to social media, including respecting the rules of the venue, striving for transparency and openness in interactions, and being respectful in all online interactions. Other policies expressed an expectation of “trust” that employees will provide professional-level comments or content whether in their professional or personal lives.

None of the policies reviewed directly address the consequences of inappropriate conduct on personal social media sites. However, outlining which aspects are simply recommendations for personal behavior and which ones are potential grounds for dismissal might be useful for employees and their managers trying to navigate and define the parameters of the personal/professional divide.

Sample language outlining employee conduct expectations when using social media

"A summary of the key points of ethical Social Media conduct are reproduced below:

- i. Customer protection and respect are paramount.
- ii. We will use every effort to keep our interactions factual and accurate.
- iii. We will strive for transparency and openness in our interactions and will never seek to “spin” information for our benefit.
- iv. We will provide links to credible sources of information to support our interactions, when possible.
- v. We will publicly correct any information we have communicated that is later found to be in error.
- vi. We are honest about our relationship, opinions, and identity.
- vii. We respect the rules of the venue.
- viii. We protect privacy and permissions."

~State of Delaware

Sample language describing standards for content created by individuals using professional accounts

"[The] lines between public and private, personal and professional are blurred. By identifying yourself as a State employee, you are creating perceptions about your expertise and about the State by legislative stakeholders, customers, business partners and the general public...Be sure that all content associated with you is consistent with your work and with the State’s values and professional standards."

~State of Utah

5. Content

The issues of who is allowed to post content on official agency social media pages and who is responsible for ensuring its accuracy came up frequently in our interviews and fourteen of the reviewed documents address content management in some way. Content management strategies range from some agencies exerting minimal editorial controls over content by allowing their employees to write freely in agency blogs on various mission related topics (e.g., US EPA), to other agencies that keep responsibility for content creation and management solely with the public information officer (e.g., City of Seattle, Washington).

In many cases, such as Fairfax County, VA, the responsibility for creating content is given to the department or individual who created the account, with the agency’s public information officer being responsible for ensuring the accuracy of the posted information and adherence to existing social media policies.

Eight Essential Elements

The question of content management with respect to an employees' professional and personal use is left largely unexplored in policy and guideline documents. However, it was a concern for many of the professionals we interviewed. Outside of official agency social media pages, these professionals are more and more engaging in work-related group discussions on sites such as GovLoop or LinkedIn and leaving online comments in response to work-related topics on external blogs. Ten of the 26 policies reviewed simply instruct their employees to always use a standard disclaimer that distances the employee's opinions and content from the official agency position.

For example, the social media policy and guidelines for the US Air Force instructs employees to specify, through a disclaimer, that any comments provided by an employee on external social media sites are personal in nature and do not represent the views of the US Air Force. In addition, while not included in their guidelines or policy documents, the US Air Force developed a flowchart designed to help airmen decide how to respond to comments from the public when they come across discussions about the Air Force on social media sites.(3)

Sample language concerning content management

"Agencies are responsible for establishing, publishing, and updating their pages on social media sites. Although it will be the agency's responsibility to maintain the content, the Office of Public Affairs will monitor the content on each of the agency pages to ensure 1) a consistent countywide message is being conveyed and 2) adherence to the Social Media Policy. The Office of Public Affairs also reserves the right to direct agencies to modify social media content based on best practices and industry norms."

~Fairfax County, VA

Sample language concerning content management

"Public Affairs will:

- Maintain the blog, including the look and feel and pages for the comment policy, blog description, etc.
- Review each post. This will primarily be for policy and legal issues; other editing will be very light, essentially only to correct spelling or grammatical mistakes.
- Coordinate review with the Office of General Counsel for legal issues."

"EPA blogging is a privilege, not a right. Because of federal and legal responsibilities, EPA management reserves the right to review blog content or to un-invite anyone to blog."

~US Environmental Protection Agency

6. Security

Governments are working to develop best practices to ensure the security of their data and technical infrastructure in light of the new uses, users, and technologies related to social media use.

Some of the reviewed policies deal explicitly with security concerns for social media, while others are more general. For instance, the City of Hampton's policy simply points to existing IT security policies by stating, "Where appropriate, City IT security policies shall apply to all social networking sites and articles." Other policies target specific security concerns; two types generally found in the policies analyzed and discussed in the interviews were technical and behavioral concerns.

The technology concerns addressed in the policies focused on password security, functionality, authentication of identity using public key infrastructures, and virus scans. Fifteen of the policies included specific requirements such as requiring users to maintain complex passwords. A few policies required a designated official to hold all username and passwords for social media accounts.

The Department of the Navy memo on social media specifically mentions following the Department of Defense's Public Key Infrastructure procedures and restricts the posting of classified information to protected sites only. Two policies detail how attachments should be scanned using anti-virus tools before they can be posted on behalf of the government.

The behavioral security concerns refer to those threats that result from employees' intentional or inadvertent actions when engaging with social media sites and tools. The *Guidelines for Secure Use of Social Media by Federal Departments and Agencies* by the Federal CIO Council discussed the two major threats that rely on

Eight Essential Elements

certain types of behaviors by users—*spear phishing* and *social engineering*. For example, employees may inadvertently post information about themselves or the agency on social media sites, which attackers then use to manipulate users. A related concern is the inadvertent posting of citizens' personal and protected information by agency employees. While these concerns are not new, many of the reviewed policies mentioned the need to protect confidential information that is personally identifiable or could endanger the agency mission.

Sample language outlining the technical concerns and processes to follow:

"Agency IT Administrators shall:

1. Limit Internet access Social Media web sites according to the agency's acceptable use policy, while allowing authorized Users to reach content necessary to fulfill the business requirements. Limitations may include:
....
 - a. . . .
 - b. Allowing Internet access to Users who are specifically authorized.
 - c. Preventing unnecessary functionality within Social Media web sites, such as instant messaging (IM) or file exchange.
 - d. Minimizing and/or eliminating the addition of web links to other web sites, such as "friends", to minimize the risk of exposing a government user to a link that leads to inappropriate or unauthorized material.
2. Enable technical risk mitigation controls to the extent possible. These controls may include:
 - a. Filtering and monitoring of all Social Media web site content posted and/or viewed.
 - b. Scanning any and all files exchanged with the Social Media web sites."

~State of California

7. Legal Issues

The use of social media tools raises the issue for many agencies about how to ensure that their employees are abiding by all existing laws and regulations. Some policies take a general approach to legal issues, using generic text that requires all employees to adhere to all applicable laws and regulations without actually specifying which laws and regulations are applicable. Others point to specific areas of law such as privacy, freedom of speech, freedom of information, public records management, public disclosure, and accessibility.

A number of policies include language outlining records management and retention schedules for content posted to social media sites. The policies that address this issue focus on retaining social media records, but a few include language related to the removal of records (for example, see bullet 6 in the City of Hampton, Virginia policy below). The State of Massachusetts highlights the transitory nature of records in its guidelines on Twitter and provides instructions on how to download Tweets from Twitter to prevent loss of content.

Some policies proactively address potential legal issues by requiring the use of various disclaimers on social media sites. One example of a standard disclaimer is for use by employees when engaging in social media activities and is intended to detach the opinions and actions of individual employees from their employer. For example, The City of Hampton, Virginia directs its employees who choose to engage citizens on social media sites on behalf of the City to "Make it clear that you are speaking for yourself and not on behalf of the City of Hampton. If you publish content on any website outside of the City of Hampton and it has something to do with the work you do or subjects associated with the City, use a disclaimer such as this: 'The postings on this site are my own and don't necessarily represent the City's positions or opinions.'" Other standard disclaimers concern public records, external links, endorsements, copyright, privacy, and offensive behavior.

Sample disclaimer for comments being treated as public records

"Posts and comments to and from me, in connection with the transaction of public business, is subject to the North Carolina Public Records Law and may be disclosed to third parties."

~State of North Carolina

Sample language outlining specific laws and impact

“All City of Hampton social networking sites shall adhere to applicable state, federal and local laws, regulations and policies including all Information Technology and Records Management City policies and other applicable City policies.

1. . . .
2. . . .
3. Freedom of Information Act and e-discovery laws and policies apply to social media content and therefore content must be able to be managed, stored and retrieved to comply with these laws.
4. City of Hampton social networking sites are subject to Library of Virginia's (LVA) public records laws. Relevant City of Hampton and (LVA) records retention schedules apply to social networking content. Records required to be maintained pursuant to a relevant records retention schedule shall be maintained for the required retention period in a format that preserves the integrity of the original record and is easily accessible using the approved City platforms and tools.
5. All social network sites and entries shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure.
6. Content submitted for posting that is deemed not suitable for posting by a City of Hampton social networking moderator because it is not topically related to the particular social networking site objective being commented upon, or is deemed prohibited content based on the criteria in Policy–Item 9. of this policy, shall be retained pursuant to the records retention schedule along with a description of the reason the specific content is deemed not suitable for posting.”

~ City of Hampton, Virginia

8. Citizen Conduct

Social media sites, unlike more traditional media such as newspaper or radio, allow for instant two-way public communication between government and citizens. Citizens are able to directly post audio, video, and text to many social media sites. Agencies must decide whether to allow two-way communication, such as the use of comment boxes, and how to handle this engagement with citizens. For agencies that decide to elicit citizen feedback via their official agency social media sites, rules for acceptable conduct of citizens are often developed.

Eleven of the 26 reviewed policies and guidelines addressed the issue of citizen conduct. The documents vary with respect to how they deal with the content of comments. Some issue rules of conduct that are posted on the agency's site. These rules generally refer to limitations on offensive language, inciting violence, or promoting illegal activity. Similar rules are often already used on agencies' websites and can be reused for social media purposes. Other policies, such as the policy of the City of Arvada, simply talk about who will have the responsibility of approving public comments without going into detail as to what makes a comment acceptable.

Sample language outlining the preferred conduct of citizens

“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

Eight Essential Elements

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).”

~City of Seattle, Washington

(3) http://www.wired.com/images_blogs/photos/uncategorized/2009/01/06/air_force_blog_char.jpg