GUIDANCE ON SOCIAL NETWORKING

Outline:
A. Records Management Considerations
B. Information Technology Considerations
C. Important Links

A. Records Management Considerations

1. For the Record

As public bodies / governments, any information created for, or received from Social Networking / Web 2.0 applications and tools will probably be a record. If the information / data meets the requirements of the definition of a "record" in Arizona Revised Statutes (A.R.S.) §41-1350, then you will need to retain such information. Any Social Networking (SocNet) records will need to be managed in a way that complies with all of the Records Management requirements found in State Statutes. (See A.R.S. §39-101, §41-1330-55)

Title 41-1350. Definition of records

> "In this chapter, unless the context otherwise requires, "records" means all books, papers, maps, photographs or other documentary materials, **regardless of physical form or characteristics**, including prints or copies of such items produced or reproduced on film or electronic media pursuant to section 41-1348, **made or received** by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor **as evidence of** the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein. Library or museum material made or acquired solely for reference or exhibition purposes, *extra copies of documents preserved only for convenience of reference* and stocks of publications or documents intended for sale or distribution to interested persons are not included within the definition of records as used in this chapter."

2. SocNet is No PicNic

The Statutory requirements regarding Records Management of public records are never easy, and that is especially so for these records. You need to be prepared for these challenges, and aware of the difficulties you will face in complying with these requirements regarding SocNet records. Our Agency is aware of these difficulties, and that is our main reason for providing this Guidance. It is our hope that you will be able to think about these issues before you decide the extent of your involvement in SocNet / Web 2.0 – and take the necessary steps to ensure successful management of these records. And remember, e-mail has been around for over 15 years and we are all still trying to find the most efficient and cost effective manner for properly managing **e-mail records**.

3. It's the Content (and Intent), Stupid

In the 1992 Presidential Election, the unofficial slogan of the Clinton Campaign was, "It's the Economy, Stupid." A potent reminder, both then and now, to not overlook the critical issue(s) facing us with any problem. With SocNet records, it really is the content that is most critical, from a Records Management point of view.

The transitory nature of most SocNet communication does not mean that any records created or received while using these tools will be transitory. It is the **content and the intent** of the communication that determines whether these communications will qualify as records, and the specific retention period required for such records. The content created or received will determine what type of record series is most appropriate for the information, and the records series will then determine the retention period needed for such records.

If the records are truly duplicates or copies being retained elsewhere, then their retention as SocNet records will be short-lived. But, in the case of comments / postings / feedback, most of this will be unique and will need to be retained per specific records series / retention periods and based upon the content of these communications.

4. No Schedule, No Service

Make sure SocNet records are on a Retention Schedule. Placing these records on a Retention Schedule will help draw attention to the fact that information created or received from these sites can be records, and require the appropriate retention as records. The ASLAPR revised the earlier "E-mail Schedule" from 2006, and expanded that Schedule to include all forms of electronic communications and social networking. The resulting General Schedule is the *Electronic Communications and Social Networking Records*, and it is an identical Schedule for all seven types of public bodies. As an example, the *All State Agencies, Boards and Commissions* Schedule can be found at the following link: http://www.lib.az.us/records/documents/pdf/state%20-%20email.pdf

5. For Once, Try NOT to be Original

Copies / duplicates of information already existing and being managed elsewhere by an Agency are Not public records, so that information will not need to be retained, or can be retained for a short period of time. (See italicize portion of A.R.S. §41-1350, above) From a Records Management point of view, you will want to set up guidelines for what topics / subjects / information can be blogged posted or networked. Try to avoid asking for public comment on policies, procedures or topics coming up for possible consideration at future Board / Council meetings. This may make such communications, "Executive Correspondence…that sets or discusses policy" and these types of records (records series) are Permanent – requiring retention on paper or microfilm.

As much as possible, ask employees to use information / data / records that already exist elsewhere in your Agency. It is much easier to manage information on your own website(s) than it is to manage pages on Facebook, or any other SocNet site. Keeping original, unique information under your direct control and posting only duplicate information to SocNet sites places you in a better position to manage your electronic records and content.

6. King of the Content

Who controls the content of these SocNet records? In most cases, the SocNet website will have full control over the content of everything posted to their sites. And, if they control the content, then they will usually control the retention of the records, therefore controlling the entire Records Management process. It is difficult to manage what you have no control over. Most SocNet sites have little to no Records Management capabilities since they view this type of communication as transitory. But remember, just because SocNet information may be viewed as temporary and casual does not mean that records created or received by SocNet are transitory; it's all about the content.

As public bodies, you will need to "manage" these records, as you would any other records. See the requirements of A.R.S. §41-1346: "*A. The head of each state and local agency shall: 1. Establish and maintain an active, continuing program for the economical and efficient management of the public records of the agency.*" The State of Arizona has approached some of the larger players in the SocNet world, and is working with these sites to incorporate controls and features needed by public bodies that have not been previously designed into these sites. The capabilities needed from a government standpoint are very different from those of the general public.

Most of the capabilities being discussed have been developed by first making these sites aware of statutory requirements for records management, security, and so on. One pending enhancement is the ability to "certify" a page as being a true "State of Arizona" Agency or Officer page. Just because a SocNet page claims to be an Arizona Agency or Elected Official does not mean it is actually the product of such. There is a need to be able to "certify" to the public that the page is not bogus, nor maliciously bent on abusing the ignorance of the visitors to such a page.

7. If you Can't, Should You?

If you can't manage the records created or received by SocNet, should you allow the use of SocNet? The Statutes require public bodies to "efficiently and effectively" manage their records, so make sure that you can properly do so before you start tweeting, blogging or posting. You may need to "turn off" certain aspects of a social networking site / application, if you are not prepared to fully manage the SocNet records generated.

This may make your SocNet site more of a one-way communication tool, but it can help prevent some of the problems associated with two-way communication sites until you are ready to handle them. For instance, if you are not prepared to manage messages posted to your page, then you should consider turning off the capability of allowing others to leave wall posts. Unfortunately, that is easier said than done with some SocNet sites.

8. E-mail Comments and Postings

Comments, wall postings, etc received by Users, Friends, Fans (and others) of your SocNet site will probably be unique records. As such, you will need to capture and retain them accordingly. Comments posted to some sites can be forwarded as an e-mail, which increases your ability to better manage these unique records. Having these comments and postings e-mailed to one of your e-mail accounts puts the control over these records back into your hands. Consider forwarding these e-mails to an Agency account, similar to those used to capture public comments made on your government websites.

Facebook does, however, offer this function, and you can learn how to do so from the blog, **April's Chatter Box.** (See the entry, "Public Records…Tools for RM Archiving of Twitter & Facebook", at the following: http://apriledmonds.wordpress.com/2009/12/10/tools/ If you are not prepared to manage the comments / postings, or the sites are not able to forward such postings to your e-mail address, you can sometimes turn off the ability of the public to post such comments.

9. Notify and Involve Information Technology (IT)

If it isn't already apparent, most Records Managers will need to partner with their Information Technology colleagues if they want to truly manage the great potential and challenges posed by SocNet. Make sure your IT professionals are able to track the use of these technologies as they do e-mail and other e-communications. Involve them by asking how you can capture, retain and manage these records. Any electronic communication requires a concerted, coordinated effort on behalf of your Records Management and IT personnel. There may already be an I.T. policy governing use of the internet and related tools and sites, but you can make sure Records Management concerns are fully addressed in these policies.

10. No Policy, No Service

Have a policy on SocNet (along with other e-communications) and focus on Records Management responsibilities and requirements. Public bodies need to know what their employees are using SocNet for, and what information is being created and / or received. This can best be done upfront, by defining the parameters of SocNet activity. Make sure your policy sets the party / parties responsible for capturing, retaining and managing these SocNet records, or you will ensure that no one is responsible.

This Guidance could be used as a great start to creating your own Records Management policy for Social Networking. If you don't want to totally reinvent the wheel, you can review over 100 Social Networking usage and / or governance policies at the following links:
Social Media Policies Database of Over 110 Organizations
http://www.socialmediatoday.com/SMC/155843

Social Media Governance Database of Over 130 Policies:
http://socialmediagovernance.com/policies.php

11. The Matrix
An essential outgrowth of either the I.T or Records Management policy for Electronic Communications and SocNet will be the matrix. You will need to create and maintain a matrix of your Agencies / Divisions / Employees use of Web 2.0 technology, best broken down by application. This matrix should include the specific technology involved, Departments involve, web address / location of each, and the opportunities / potential for each. See an example of the excellent Federal government matrix at the following US.gov link: http://www.usa.gov/webcontent/documents/Web_Technology_Matrix.pdf

12. If it Works, Use It
Control SocNet activities from the very beginning. One of the best ways to ensure that the use of SocNet sites and tools is going to be acceptable to your public body is to provide guidance and assistance when the SocNet pages are first being set up. Consider developing a Tool Kit, or even creating a SocNet page that teaches your Agencies / Departments how to set up a SocNet account / page of their own.

See either the State of Florida or the Federal Government toolkits at the following sites:
State of Florida: http://sites.google.com/site/flsocmed/
(You need to click the links at the bottom of the page to get more information on "Lessons Learned", "Twitter", "Video", etc.)
Federal Government: http://www.usa.gov/webcontent/technology/other_tech.shtml

13. Use the Terms
What do you do if someone in the public posts a message to your SocNet site that is offensive or obscene? Do you immediately remove the post and delete the record? Do you allow the post to remain on your wall? Do you remove the post but retain it at a secure portion of your site? Remember that post to a government SocNet site are probably going to meet the statutory definition of a record, and must be managed accordingly.

Consider incorporating the Terms of Use established by the venue for your SocNet activities into your Policy. These Terms of Use already define ones participation in SocNet, so why not reflect them in your policy? In most cases, these Terms of Use will address issues such as profanity, intellectual property and / or copyright infringement, and other difficult issues. Most users of SocNet sites will be familiar with the need to both know and comply with the Terms of Use, and will not find it unusual that your public body SocNet site has incorporated these Terms into your policy, procedures or practices.

14. Keep It Simple

Try to keep communications / blogs to a single topic, since this will make it easier to manage these records. Retention Schedules are built around managing records according to one specific retention period for each specific records series / type. Mixing multiple topics in your SocNet communications will make it that much more difficult to determine the correct retention period for these records. In addition, be aware of the subjects that require longer retention, and try to avoid these. (Remember that "Executive Correspondence… that sets or discusses policy" is a Permanent record and, as such, cannot be retained electronically.) It is probably best to discourage your executives from having "correspondence" with the public about established, pending or potential policies.

15. Use a Title / Heading

Whenever and wherever possible, use a title or heading for your information, since this will help with managing these records. (Similar to the subject line for e-mail.) Most government employees familiar with e-mail and other forms of electronic communications will be acquainted with such a header / subject line, and will be more likely to use one. Make sure the title / heading of your posting / entry accurately describes the content and / or intent of your information.

The heading used will help guide those tasked with retaining these records. If your blog article is titled, *Social Networking From a Records Perspective*, it will be easier to determine the retention period and manage the record accordingly. If you are not required to manage your own SocNet sites, then making use of a heading or title will help others know how best to categorize these records on the Retention Schedule, thereby guaranteeing the proper retention period.

16. Train, Train, Train

You can never train too much on the Records Management aspects of SocNet and other forms of electronic communication. Training is an important aspect of any compliance program, and is a sure line of defense for any public body. Remember the four pillars of an effective Records Management Program – Retention Schedules, RM Policies, Training and Documentation.

What should you train your employees on when it comes to SocNet**?** Take some wise advice from the Feds - The following is an excerpt from the September 2009, Federal CIO Council publication, *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*. This section focuses on what governments should incorporate into employee training on SocNet, and offers some great advice on things we should be aware of.

a. "Users are almost always the weakest link in an information system, and may inadvertently divulge sensitive information through a social network. Few effective technical security controls exist that can defend against clever social engineering attacks[19]. **Often the best solution is to provide periodic awareness and training of policy, guidance, and best practices.** The proper use of social media in the Federal Government should be part of annual security awareness training, and address the issues below.

b. Provide specialized training to educate users about **what information to share, with whom they can share it, and what not to share**. For an example of establishing departmental policy on what to share on social media websites, see the United States Air Force New Media Guide[9].

c. Provide guidance and training **based on updated agency social media policies and guidelines**, including an updated Acceptable Use Policy (AUP) specific to social media websites.

d. Provide guidance to employees to **be mindful of blurring their personal and professional life**. Don't establish relationships with working groups or affiliations that may reveal sensitive information about their job responsibilities.

e. Provide Operations Security (OPSEC) awareness and training to educate users about the **risks of information disclosure when using social media, and make them aware of various attack mechanisms** as described in this document.

f. Provide federal employees with additional **guidance concerning if and how they should identify themselves on social media websites, depending on their official role**.

g. Provide specialized awareness and training on Privacy Act requirements and restrictions. **Educate users about social networking privacy controls to help them take control of their own privacy**, both in their personal profile and any profile they use for work-related activities.

h. Educate users about **specific social media threats before they are granted access to social media websites**. Users may be desensitized to openly granting unnecessary access to their private information. For example, users may click "OK" without reading the full message and understanding the permissions they are granting."
(Guidelines for Secure Use of Social Media by Federal Departments and Agencies, September 2009)

B. Information Technology Considerations

8 Essential Elements for an Effective Government Social Networking Policy
Government Technology magazine / webzine, May 25, 2010, By Karen Wilkinson, Staff Writer

While government agencies keep evolving to "meet citizens where they are" by joining social media sites, creating policies that allay the risks such tools pose can be an arduous, convoluted task.

"Creating a policy for the use of social media policy by a government agency is not a simple task," states a recent study from the Center for Technology in Government (CTG) at the University at Albany, State University of New York. "One not only has to contend with an ever-changing landscape of the social media environment, but also with the various ways governments employees are using these tools to do their work."
While there are many examples of government agencies effectively engaging citizens via social media tools, these best practices remain relatively new and unexplored for the majority of governments nationwide, according to the study.

"What we've noticed is there's a lot of fears, questions and concerns related to social media use," said CTG Program Associate Jana Hrdinová. "We try to take these fears and concerns and classify them into manageable areas -- to make it easy to follow through all the various questions and not get lost in the process."
In a study of 26 publicly available government social media documents, along with results from interviews with 32 government professionals already using or considering using social media tools, the CTG winnowed its findings down to eight essential elements to address for the use of social media.

Those eight elements include employee access, account management, acceptable use, employee conduct, content, security, legal issues and citizen conduct. While these elements don't cover every possible issue (the guide is part of a larger project under way that focuses on government use of social media tools), it's a jump-off point:

1. Employee Access

Not long ago, social media sites fell under the "non-work-related" umbrella, and thus governments tended to restrict access to these areas of the Internet. But those lines have blurred lately as personal, professional and official agency use of social media tools has become common, raising questions about whether employees should have access to social media sites and the proper means for gaining access.

Agencies are managing access in two ways: controlling the number and type of employees allowed access to social media sites or limiting the types of sites that are approved for employee access. Most agencies interviewed by the CTG restricted access to such sites, instead allowing access for only a handful of designated individuals or functions (such as leadership or public information officers).

But formal policies that specifically address access appear lacking: Of the 26 policies and guidelines CTG reviewed, only five specify access procedures. "Of those five, most required employees or departments to submit an official business case justification in order to access and use social media sites," the study said.

Based on its interviews, balancing unrestricted and controlled access is 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 are still fearful of the perceived legal and security risks," the study said.

2. Account Management

This entails the creation, maintenance and potential destruction of social media accounts. Lacking a policy for this could result in a situation where an agency's leadership is in the dark about what types of accounts are being established, maintained or closed by their employees for professional or official agency use, according to the study. In policies reviewed by the CTG, such strategies varied. One strategy required approval by only one

designated party (most often the public information officer), while other agencies require approval by more than one party.

"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," the study said.

3. Acceptable Use

Such policies usually outline an organization's position on how employees are expected to use agency resources, restrictions on personal use and consequences of violating the policy. Twelve of the policies and guidelines reviewed by the CTG dealt with this specific issue, and the majority of them used existing policies that already dictated acceptable use of common electronic and information resources such as telephone, computer or Internet access.

This is perhaps one of the more disquieting, gray areas of social media policy, Hrdinová said, as it's difficult to make clear-cut distinctions between professional and personal use. For example, an employee may be Facebook friends with a CIO from another agency and chat in person and online about common interests, which may ebb and flow without much distinction from personal to professional. "But at the same time, are they strengthening the professional relationship?" she asks.

To illustrate the lack of policies surrounding acceptable personal use during designated times or nonwork hours, the CTG found that only three of the 26 policies have started addressing the issue.

For some agencies, the line isn't so blurry: Arvada, Colo., has a social media policy that clearly states, "Social media use is for corporate goals and objectives, not for personal use."

Others, like the U.S. Air Force, have more lenient policies and encourage their members to think of themselves as on duty 24/7 when it comes to social media use. Others suggested "acceptable employee use for professional interest is better monitored and managed by supervisors, rather than a one-size-fits-all policy.

4. Employee Conduct

Most agencies reference existing policies by either using direct quotes or providing links or reference numbers on specific policies that address what is "right" and "wrong" as far as employees' behavior, and sets out consequences should a violation occur. However, none of the reviewed policies directly address the consequences of inappropriate conduct on personal social media sites, the CTG said.

In addition to standard conduct codes that address issues like racially offensive language, some policies 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," the study said.

While creating policies to address consequences of inappropriate use of social media tools is largely untouched territory, outlining which aspects are just recommendations for personal behavior and which 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," the study said.

5. Content

Issues of who is allowed to post content on official agency social media sites and who is responsible for its accuracy came up frequently in the CTG's interviews. Fourteen of the reviewed documents address content management in some form. In many cases, such as Fairfax County, Va., content creation is given to the department or person who created the account, with the agency's public information officer being responsible for ensuring the accuracy of posted information and adherence to existing social media guidelines. But "the question of content management with respect to an employees' professional and personal use is left largely unexplored in policy and guideline documents," the study said.

More and more, professionals are engaging in work-related group discussions on sites like GovLoop and LinkedIn, and leaving online comments in response to work-related topics on external blogs, another concern for agencies. Ten of the 26 policies 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 Air Force's social media policy and guidelines instruct 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 Air Force.

6. Security

Agencies are trying to develop best practices to ensure security of their data and technical infrastructure in light of new uses, users and technologies related to social media. Some of the 26 policies deal explicitly with social media security concerns, while others are more general. For example, the Hampton, Va., policy points to existing IT security policies by stating, "Where appropriate, city IT security policies shall apply to all social networking sites and articles."

Others target specific concerns: Two types generally found in the policies analyzed and discussed in interviews were technical and behavioral concerns. 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, and a few policies required a designated official to hold all usernames and passwords for social media accounts. As well, two policies detail how attachments should be scanned using anti-virus tools before being posted on behalf of the government.

Public-sector employees also 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," the study said.

7. Legal Issues

While some agencies' policies take a general approach to legal issues -- using generic text that requires all employees to adhere to applicable laws and regulations without specifying which are applicable -- others point to specific areas of law like privacy, freedom of speech, freedom of information, public records management, public disclosure and accessibility. Many agencies address the issue of records management and retention, but few include language related to the removal of records. Massachusetts, however, highlights the transitory nature of records in its guidelines on Twitter and gives instructions on how to download tweets from Twitter to prevent content loss.

Some agencies' policies proactively address potential legal issues by requiring using various disclaimers on social media sites like Hampton which directs its employees who engage on behalf of the city to "make clear that you are speaking on behalf 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.'"

8. Citizen Conduct

Grappling with instant two-way public communication between government and citizens is relatively new, and agencies must decide whether to allow such communication like comment boxes and how to handle that engagement. "For agencies that decide to elicit citizen feedback via their official agency social media sites, rules for acceptable conduct of citizens are often developed," the study said.

Eleven of the 26 policies and guidelines addressed this issue. Documents vary on how to deal with the content of such comments. "Some issue rules of conduct that are posted on the agency's site," the study said. "These rules generally refer to limitation on offensive language, inciting violence or promoting illegal activity. Similar rules are often already on agencies' websites and can be reused for social media purposes." But some policies, like Arvada's, simply detail who will have the responsibility of approving public comments without going into detail as to what makes a comment acceptable.

On top of the eight elements to effectively design a government social media policy, the CTG offers further guidance for those governments that are just getting started, including determining goals and objectives, forming a team, identifying existing policies that apply to using social media tools and discussing conflicts or inconsistencies between proposed, and existing policies and procedures.

(*8 Essential Elements for an Effective Government Social Networking Policy,* By Karen Wilkinson, **Government Technology** magazine / webzine, May 25, 2010,)

C. Important Links (accurate as of 06/15/2010):

1. Why Governments Need a "How-to Toolkit" When Using Social Media / Social Networking:
http://www.govtech.com/gt/765118

2. State of Florida Toolkit for "How to Use" Social Media / Social Networking Tools:
http://sites.google.com/site/flsocmed/
You need to click the links at the bottom of the page to get more information on "Lessons Learned", "Twitter", "Video", etc.

3. Federal Government's Toolkit for Web 2.0 and Social Networking:
http://www.usa.gov/webcontent/technology/other_tech.shtml

4. State of Arizona Policy on Social Networking:
http://www.azgita.gov/policies_standards/pdf/P505%20Social%20Networking%20Policy.pdf

5. Tools for RM Archiving of Twitter & Facebook:
http://apriledmonds.wordpress.com/2009/12/10/tools/

6. Social Media Policies Database of Over 110 Organizations
http://www.socialmediatoday.com/SMC/155843

7. Social Media Governance Database of Over 130 Policies:
http://socialmediagovernance.com/policies.php

8. United States Air Force, Web Posting Response Assessment:
http://www.af.mil/shared/media/document/AFD-091210-037.pdf