

Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions

December 23, 2008

Produced by the following members of the Federal Web Managers Council:

Bev Godwin, GSA/USA.gov (Executive sponsor)

Sheila Campbell, GSA/USA.gov (Co-chair)

Jeffrey Levy, EPA (Co-chair, Social media sub-council)

Joyce Bounds, Dept. of Veterans Affairs (Co-chair, Social media sub-council)

A. The context for using social media within the federal government

As leaders of the Federal Web Managers Council, we've seen that social media in government has become the number one topic of discussion within our government web manager community over the past year. The prospect of agencies using social media sites such as YouTube, Facebook, Wikipedia, Twitter, and SecondLife has raised a myriad of legal, contractual, and policy questions. As the new Administration looks to leverage these new tools to create a more effective and transparent government, it's an opportune time for us to share what we've learned and propose solutions for how to best use these new tools across government. These recommendations are based on our first-hand experience using social media within our own agencies and from hundreds of conversations with web managers across the country.

Some agencies are already using social media tools with great success. They've shown how these tools can transform how we engage the public, include people in the governing process, and accomplish our agency missions. (See [WebContent.gov](http://www.usa.gov/webcontent/technology/other_tech.shtml) for examples of agencies successfully using social media: http://www.usa.gov/webcontent/technology/other_tech.shtml). But many agencies are not using these tools, either because of perceived or real lack of resources, cultural resistance, or legal or other barriers. There are varying interpretations around what is allowed across the federal government, and some agencies do not yet understand how these tools will help them achieve their missions.

The purpose of these recommendations is to address the perceived and real barriers to using social media, and to propose solutions that will result in greater consistency and a clearer understanding of what is expected and permitted across federal agencies.

We hope this paper will facilitate dialogue on these important issues, both within and outside the government. As this topic evolves, we'll use [Webcontent.gov](http://www.usa.gov/webcontent/) and various social media tools to continue the conversation. We also invite you to read the Federal Web Managers Council white paper, "[Putting Citizens First: Transforming Online Government](#)," which offers recommendations for transforming online government beyond social media (http://www.usa.gov/webcontent/documents/Federal_Web_Managers_WhitePaper.pdf).

B. Barriers and potential solutions

1. Cultural issues and lack of a strategy for using these new tools

Issue: Many agencies view the use of social media as a technology issue, instead of a communications tool, and management decisions are often based solely on technology considerations. In many cases, the focus is more on what can't be done rather than what can be done. The default approach should be openness and transparency. For this reason, agencies need to be prepared that the decision to use social media will have cultural implications throughout government. Some agencies have leadership and legal support and have shown that the benefits of using social media outweigh the risks; but many have not. The result: social media is not consistently applied across government.

Proposed Solution: The new Administration should communicate a government-wide strategy for using social media tools to create a more effective and transparent government. The new Administration's Chief Technology Officer (CTO) should require each agency to, within three months, develop their own social media/Web 2.0 communications strategy that describes how it will use their agency website and the larger Web to accomplish its mission, reach new audiences, and engage the public. The strategy should include resources needed to accomplish these goals.

2. Employee access to online tools

Issue: Many agencies block their employees from using sites like YouTube, Facebook, and Wikipedia. They make one of three arguments, all of which can be addressed through effective policies and management controls:

1. **Security:** IT security specialists raise concerns that these high traffic sites pose a greater risk for malware and spyware. However, agencies can implement security measures to mitigate these risks, just as they do for other high traffic sites such as Google and Yahoo. Certain agencies may still need to restrict access for specific groups, but this should be the exception, not the rule.
2. **Employees will waste time:** this is the same argument that has been used to say employees shouldn't have access to phones, email, etc. It's not unique to Web 2.0. It should be addressed by agency managers as a management issue, not a technology problem.
3. **Bandwidth:** this is a legitimate concern for sites such as YouTube that consume considerable bandwidth. However, agencies need to budget for this, as they do for other infrastructure needs. If opening all computers to all sites is an issue, agencies should at least provide access to agency staff that need to understand and use these tools to communicate with the public.

Proposed solution: The new Administration should require agencies to provide access to social media sites unless the agency head justifies blocking certain employees or certain sites.

3. Terms of service

Issue: Most online sites require account owners to agree to terms of service that federal agencies can't agree to, in particular:

1. **Indemnification and defense:** if a federal employee, on behalf of their agency, creates an account on a social media site, they 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. Under the Anti-deficiency Act, federal agencies can't commit to either provision.
2. **Applicable law and court jurisdiction:** most terms of service also assert that a certain state's laws (usually California) apply to the terms of use and that the state's courts will adjudicate disputes. This is problematic since federal agencies follow federal law and go to trial in federal court.

Many companies have been willing to negotiate on these issues, but they don't want to negotiate separate agreements with dozens of different agencies. Similarly, it's not efficient for agencies to work out agreements with an unending list of potential companies.

Proposed solution: The new Administration (through the National CTO, GSA, OMB, or some other central organization) should:

- a) Establish a single terms of service that covers all social media sites, which excludes the federal government from the provisions described above. (If this isn't possible, at a minimum, create a standard federal terms of service with each site and establish a process for adding new agreements as new sites are identified.)
- b) Alert federal agencies that the benefits of using these sites outweigh the risks and that they should use social media sites pending agreements on terms of service.

4. Advertising

Issue: Many vendor sites place ads on all their pages; this is how they earn money from free accounts. For some agencies, this raises ethical concerns when government content appears near inappropriate

advertisements (pornography, hate, political, etc), because it can give the appearance that the government is endorsing the content. What constitutes "advertising" is interpreted differently across government.

Proposed solution: The new Administration should:

1. Issue a memo stating that government agencies should accept this kind of contextual advertising as a byproduct of using social media sites, that advertising online is no different than advertising in a magazine, newspaper, radio, or TV, where you can't control exactly how your content will appear in context. However, if this is not possible:
2. Set criteria for all agencies for when such ads are acceptable. For example, ads could be acceptable when:
 - They are ubiquitous, appearing on all similar pages on a site, regardless of the account owner
 - They do not include pornography or violence
 - There isn't confusing language that implies endorsement by the account owner (e.g., "promoted" or "sponsored" material)

5. Procurement

Issue: Government procurement rules didn't anticipate the flood of companies offering free tools to anyone who wants to use them. Attorneys at different agencies interpret the rules differently, leading to confusion and hesitation. Agencies that want to use these tools face three issues:

1. Gratuitous services and gift authority: there are rules governing when agencies are allowed to accept free services or gifts. Some agencies have gift authority and others don't. Potential concerns include giving the offering company inappropriate inside information that lets it tailor a later commercial product or possibly coming back later and billing the government.
2. Choosing winners without competition: the government shouldn't arbitrarily decide which companies will be given the cachet of providing our content, which can provide value to their sites. For example, federal agencies should have criteria to determine which video sharing sites they will publish their videos to (YouTube, Yahoo Video, AOL Video, etc).
3. Contract authority: Ordinarily, only specific employees are given authority to bind an agency contractually. This is very cumbersome when trying to establish accounts on social media sites.

Proposed solution: The new Administration should work with procurement and ethics attorneys to ensure that:

1. Agencies can use free Web products and services.
2. Agencies do not need to use all products and services offered, as long as they have criteria for deciding which ones they use.
3. Employees with a clear business need can create accounts to use free services, as long as they have managerial approval.

6. Privacy

Issue: There is no guarantee that social media sites will protect people's privacy to the same degree as federal agencies.

Proposed solution: The new Administration should direct agencies to use a standard disclaimer to display on social media sites where they publish content (i.e. EPA's Facebook page or Twitter page). The disclaimer would alert the public that they are no longer on a federal site and that the private sector site's own privacy policy applies, with a link to that policy.

7. Persistent Cookies

Issue: Agencies are banned from using persistent cookies without approval from their agency head, which effectively means the federal government isn't using them. This greatly limits our ability to serve customers' needs because our sites can't remember preferences or settings. It also means we can't take advantage of sophisticated web services and analytic tools that rely on persistent cookies.

Proposed solution: The National CTO or OMB should immediately rescind the previous guidance prohibiting persistent cookies and replace it with guidance that allows agencies to use persistent cookies to better serve customers' needs. The new guidance should state that it's acceptable for agencies to use social media sites that rely on persistent cookies. However, the government should retain the ban on tracking cookies, since they specifically track where visitors go between sites.

8. Surveys

Issue: The Paperwork Reduction Act, subsequent OMB regulations, and OMB draft guidance require that agencies complete a lengthy process to obtain an OMB control number to survey and request information from the public. This requirement is interpreted by most agencies to include voluntary online surveys, polls, and other applications that are intended to improve customer service. The Act predated the Internet and doesn't anticipate the use of social media and other customer service tools.

Proposed solution: The National CTO or OMB should issue immediate guidance that outlines exceptions to the PRA, such as using online surveys to solicit public opinion about federal websites, using social media to have online discussion forums with the public, etc.

9. Access for people with disabilities

Issue: Under section 508 of the Rehabilitation Act of 1973, all information provided to the public via agency websites must be equally accessible to people with and without disabilities. Many social media tools are automatically accessible because they are primarily text (e.g., blogs). However, some multimedia sites do not currently provide the opportunity to include transcripts or captioning, and many agencies lack sufficient resources to provide these services on their own.

Proposed solutions:

1. The National CTO should issue guidance requiring agencies to post their materials in accessible formats on their own websites, and that non-governmental sites may not be the sole location where content is posted. This will ensure that people with disabilities always have an accessible version of the content, and that the official version of content is located on a government website.
2. The National CTO and GSA should collaborate on developing a government-wide procurement vehicle to purchase tools that assist with 508 compliance, such as captioning software to make videos and webcasts available to people with disabilities.
3. The National CTO should work with major companies to make Web software, including social media software, fully accessible to people with disabilities.

10. Administrative requirements during rulemaking

Issue: The Administrative Procedure Act (APA) of 1946 sets rules for how agencies can communicate with the public during rulemaking, accept public comment on proposed regulations, etc. The Act didn't anticipate the collaborative tools now available, leading to hesitation and confusion as to how to incorporate them during the rulemaking process.

Proposed solution: The National CTO or OMB should issue guidance to help agencies use collaborative social media tools to enhance the rulemaking process, while still complying with the APA.

We welcome your questions and comments. Please contact the Federal Web Managers Council co-chairs, Sheila Campbell (sheila.campbell@gsa.gov) and Rachel Flagg (rachel.flagg@hud.gov).

[News](#) > [News Releases](#) > 2011

FOR IMMEDIATE RELEASE

[back](#)

January 05, 2011

OLYMPIA...Attorney General Rob McKenna announced today that Facebook has agreed to improve its terms and conditions for state and local government agencies using the social media Web site. The new terms, facilitated through the National Association of Attorneys General (NAAG) and the National Association of State Chief Information Officers (NASCIO), resolve a series of legal issues that were caused by the site's standard terms of service agreement.

"Facebook provides a tremendous venue for state agencies and their local counterparts to keep their constituents apprised of the great work that they do," McKenna said. "We and our partner agencies use the site as a means of informing the community about the work of our offices and encouraging people to become involved in their government."

With regard to McKenna's announcement, Facebook has modified portions in its terms of service agreement that all users must comply with in order to use the site.

The multistate group, led by the Colorado and Washington Attorney General's offices, began working on these modifications nearly a year ago, after the public agencies encountered a series of issues while trying to use the site.

These new terms mirror, in many ways, a similar agreement that the social media company reached with the federal government more than a year prior, which allowed 33 federal government agencies to connect with their constituents through Facebook.

Facebook has specifically agreed to modify the provisions of its terms and conditions to:

- Strike the indemnity clause except to the extent indemnity is allowed by a state's constitution or law;
- Strike language requiring that legal disputes be venued in California courts and adjudicated under California law;
- Require that a public agency include language directing consumers to its official Web site prominently on any Facebook page; and
- Encourage amicable resolution between public entities and Facebook over any disputes.

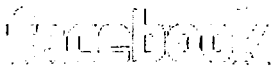
The modifications will immediately apply to state and local government agencies already on Facebook.

The states that participated in the multistate negotiations were Alaska, Arkansas, Colorado, Connecticut, Delaware, Idaho, Massachusetts, Mississippi, North Dakota, Ohio, Oklahoma, Oregon, South Carolina, Utah and Washington.

The Washington State Attorney General's Office also serves on the Washington State Social Media Working Group to help develop social media policy and best practices for all Washington state agencies. Recently, the Washington State Attorney General's Office won a "Waggy" award from the Conference of Western State Attorneys General for its social media.

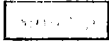
-30 -

Contacts: Janelle Guthrie, Communications Director, (360) 586-0725



Keep me logged in

[Forgot your password?](#)



Facebook helps you connect and share with the people in your life.

Government Terms

Amended Pages Terms for State & Local Governments in the United States

If you are a state or local government or government agency in the United States ("You"), and You are using Facebook Pages in your official capacity ("Official Use"), the following terms apply solely to such use and all other terms remain in effect:

1. Disputes

You and Facebook will endeavor to resolve any disputes in an amicable fashion.

2. Venue

Section 15.1 of the SRR does not apply to your Official Use.

3. Governing Law

Section 15.1 of the SRR does not apply to your Official Use.

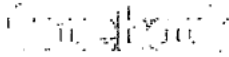
4. Indemnity

If you are a state government or state government agency in the United States:
Section 15.2 of the SRR will apply to You only to the extent expressly permitted by your jurisdiction's laws.

If you are a local government or local government agency in the United States:
Section 15.2 of the SRR will apply to You only to the extent permitted by your jurisdiction's laws.

5. Disclaimer Requirement

If you have an official website, your Page must contain, in a prominent location: "If you are looking for more information about [Government Entity], please visit [website URL]."


 Keep me logged in

 Forgot your password?

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: April 26, 2011.

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement") derives from the Facebook Principles, and governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement.

1. Privacy

Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.

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
- 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.
 - 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).
 - When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and Platform Page.)
 - When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
 - 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).

3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments.

- You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.
- You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
- You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
- You will not upload viruses or other malicious code.
- You will not solicit login information or access an account belonging to someone else.
- You will not bully, intimidate, or harass any user.
- You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
- You will not develop or operate a third-party application containing alcohol-related or other mature content (including advertisements) without appropriate age-based restrictions.
- You will follow our Promotions Guidelines and all applicable laws if you publicize or offer any contest, giveaway, or sweepstakes ("promotion") on Facebook.
- You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
- You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack.
- You will not facilitate or encourage any violations of this Statement.

4. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

- You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
- You will not create more than one personal profile.
- If we disable your account, you will not create another one without our permission.
- You will not use your personal profile for your own commercial gain (such as selling your status update to an advertiser).
- You will not use Facebook if you are under 13.
- You will not use Facebook if you are a convicted sex offender.
- You will keep your contact information accurate and up-to-date.
- You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
- You will not transfer your account (including any page or application you administer) to anyone without first getting our written permission.
- If you select a username for your account we reserve the right to remove or reclaim it if we believe appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. Protecting Other People's Rights

We respect other people's rights, and expect you to do the same.

- You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
- We can remove any content or information you post on Facebook if we believe that it violates this Statement.
- We will provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
- If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
- If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
- You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Wall and 32665), or any confusingly similar marks, without our written permission.
- If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
- You will not post anyone's identification documents or sensitive financial information on Facebook.

9. You will not tag users or send email invitations to non-users without their consent.
6. Mobile
 1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging fees, will still apply.
 2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
 3. You provide all rights necessary to enable users to sync (including through an application) their contact lists with any basic information and contact information that is visible to them on Facebook, as well as your name and profile picture.
7. Payments and Deals
 1. If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.
 2. If purchase a Deal, you agree to our Deals Terms.
 3. If you provide a Deal or partner with us to provide a Deal, you agree to the Merchant Deal Terms in addition to any other agreements you may have with us.
8. Special Provisions Applicable to Share Links

If you include our Share Link button on your website, the following additional terms apply to you:

1. We give you permission to use Facebook's Share Link button so that users can post links or content from your website on Facebook.
 2. You give us permission to use and allow others to use such links and content on Facebook.
 3. You will not place a Share Link button on any page containing content that would violate this Statement if posted on Facebook.
9. Special Provisions Applicable to Developers/Operators of Applications and Websites.

If you are a developer or operator of a Platform application or website, the following additional terms apply to you.

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our [Facebook Platform Policies](#) and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
 1. You will only request data you need to operate your application.
 2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application.
 3. You will not use, display, share, or transfer a user's data in a manner inconsistent with your privacy policy.
 4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
 5. You will not include data you receive from us concerning a user in any advertising creative.
 6. You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
 7. You will not sell user data. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer user data outside of your application.
 8. We can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations.
 9. We can limit your access to data.
 10. You will comply with all other restrictions contained in our Facebook Platform Policies.
3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on Facebook.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Facebook Platform Policies.
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
 1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
 2. comply with the Video Privacy Protection Act ("VPPA"), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.
15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, profiles, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. Special Provisions Applicable to Advertisers

You can target your specific audience by buying ads on Facebook or our publisher network. The following additional terms apply to you if you place an order through our online advertising portal ("Order"):

1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available. When serving your ad, we do our best to deliver the ads to the audience you specify, although we cannot guarantee in every instance that your ad will reach its intended target.
2. In instances where we believe doing so will enhance the effectiveness of your advertising campaign, we may broaden the targeting criteria you specify.
3. You will pay for your Orders in accordance with our Payments Terms. The amount you owe will be calculated based on our tracking mechanisms.
4. Your ads will comply with our Advertising Guidelines.
5. We will determine the size, placement, and positioning of your ads.
6. We do not guarantee the activity that your ads will receive, such as the number of clicks you will get.
7. We cannot control how people interact with your ads, and are not responsible for click fraud or other improper actions that affect the cost of running ads. We do, however, have systems to detect and filter certain suspicious activity, learn more here.
8. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for

those ads.

9. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
10. We can use your ads and related content and information for marketing or promotional purposes.
11. You will not issue any press release or make public statements about your relationship with Facebook without written permission.
12. We may reject or remove any ad for any reason.
13. If you are placing ads on someone else's behalf, we need to make sure you have permission to place those ads, including the following.
 1. You warrant that you have the legal authority to bind the advertiser to this Statement.
 2. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. Special Provisions Applicable to Pages

If you create or administer a Page on Facebook, you agree to our Pages Terms.

13. Amendments

1. We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and become a fan.
2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you a minimum of seven days notice. All such comments must be made on the Facebook Site Governance Page.
3. If more than 7,000 users comment on the proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.
4. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.

14. Termination

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 14-18.

15. Disputes

1. You will resolve any claim, cause of action or dispute ("claim") you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim.
3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR." WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS (\$100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

16. Special Provisions Applicable to Users Outside the United States

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users outside the United States.

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website.
3. Certain specific terms that apply only for German users are available here.

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; (c) social plugins such as the like button, the share button and other similar offerings and (d) other media, software (such as a toolbar), devices, or networks now existing or later developed.
2. By "Platform" we mean a set of APIs and services that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions you take.
4. By "content" we mean anything you post on Facebook that would not be included in the definition of "information."
5. By "data" we mean content and information that third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available to us (such as by using an application).
7. By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
9. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.

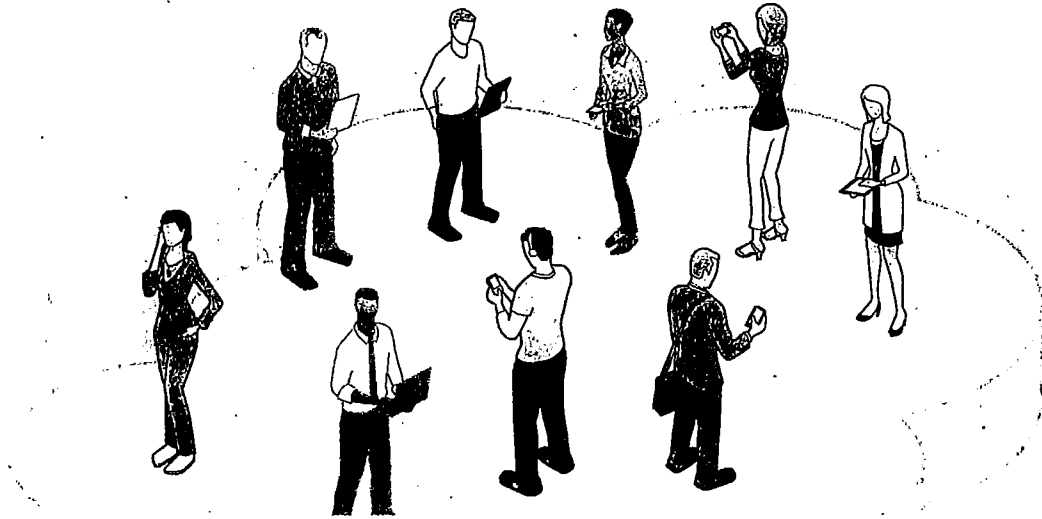
18. Other

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.
10. You will comply with all applicable laws when using or accessing Facebook.

You may also want to review the following documents:

- **Privacy Policy:** The Privacy Policy is designed to help you understand how we collect and use information.
 - **Payment Terms:** These additional terms apply to all payments made on or through Facebook.
 - **Platform Page:** This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
 - **Facebook Platform Policies:** These guidelines outline the policies that apply to applications, including Connect sites.
 - **Advertising Guidelines:** These guidelines outline the policies that apply to advertisements placed on Facebook.
 - **Promotions Guidelines:** These guidelines outline the policies that apply if you have obtained written pre-approval from us to offer contests, sweepstakes, and other types of promotions on Facebook.
 - **How to Report Claims of Intellectual Property Infringement**
 - **How to Appeal Claims of Copyright Infringement**
 - **Pages Terms**
- To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the Language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

Using Online Tools to Engage—and be Engaged by—The Public



Matt Leighninger
Deliberative Democracy Consortium

Ten Tactics for Engaging the Public

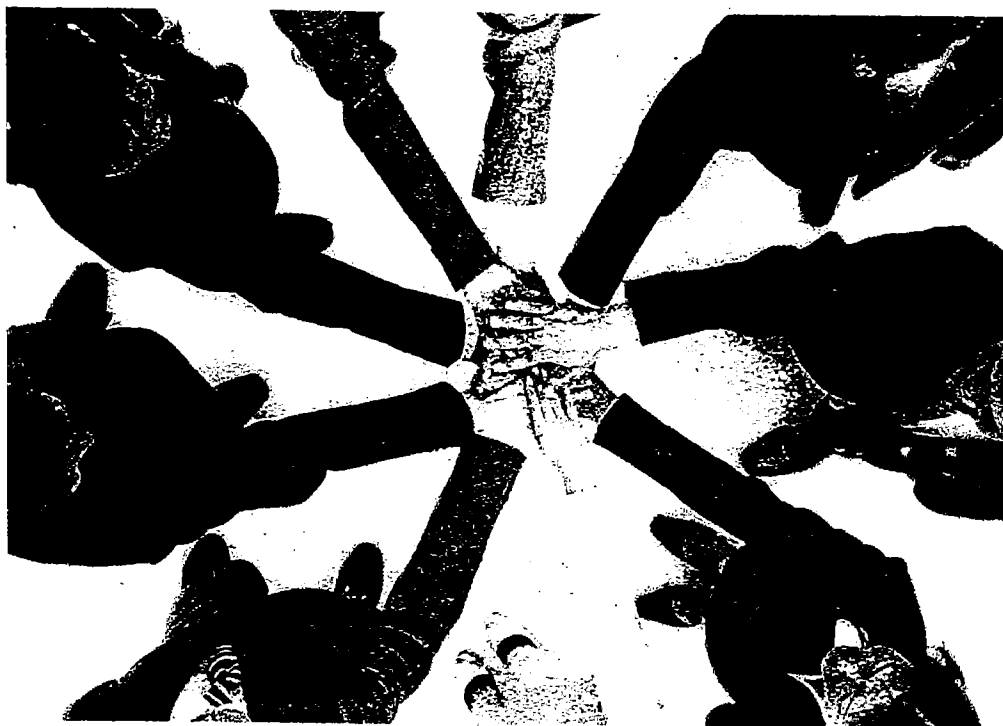
Tactic	Why Do It?	Online Tools
Collaboration		
1. Develop documents collaboratively via Wikis (Wikis)	You are trying to encourage citizens to take shared ownership of an issue and participate in addressing it	<ul style="list-style-type: none"> Wikispaces, free at basic level: www.wikispaces.com Wikiplanning,™ fee for service: www.wikiplanning.org
2. Create shared work space for citizens (Shared Workspace)	You are trying to encourage citizens to take shared ownership of an issue and participate in addressing it	<ul style="list-style-type: none"> Google Docs, free: docs.google.com Dropbox, free at basic level: www.dropbox.org GoogleGroups, free: www.googlegroups.com Ning, fee for service: www.ning.com BigTent, fee for service: www.bigtent.com CivicEvolution, fee for service: www.civicevolution.org
3. Facilitate large-scale deliberation online (Large-scale Deliberation)	<ul style="list-style-type: none"> You are in the midst of a high-profile situation in which people do not agree about what should be done You are trying to encourage citizens to take shared ownership of an issue and participate in addressing it You are trying to educate and inform citizens about a particular issue or decision 	<ul style="list-style-type: none"> Ascentum Choicebook,™ fee for service: www.ascentum.ca DialogueApp, fee for service: www.dialogue-app.com Zilino: www.zilino.com Microsoft TownHall, fee for service: www.microsofttownhall.com IBM MiniJam and InnovationJam, fee for service: www.ibm.com/ibm/jam/
4. Use "serious games" to generate interest, understanding, and input (Serious Gaming)	You are trying to educate and inform citizens about a particular issue or decision	<ul style="list-style-type: none"> Second Life, free at basic level: www.secondlife.com Zynga, fee for service: www.zynga.com Persuasive Games, fee for service: www.persuasivegames.com

Ten Tactics for Engaging the Public (continued)

Tactic	Why Do It?	Online Tools
Survey Attitudes		
5. Survey citizens	You want the immediate opinions of citizens	<ul style="list-style-type: none"> SurveyMonkey, free at basic level: www.surveymonkey.com SurveyConsole, free at basic level: www.surveyconsole.com SurveyGizmo, fee for service: www.surveygizmo.com
6. Aggregate opinions expressed on social media networks (Aggregate Opinions)	You want the immediate opinions of citizens	<ul style="list-style-type: none"> ThinkUp, free: www.thinkupapp.com CitizenScape, fee for service: www.citizenscape.net Business Analytics, fee for service: www.ibm.com/software/analytics/ COBRA, fee for service: www.almaden.ibm.com/asr/projects/cobra/
Prioritize Options		
7. Gather and rank ideas and solutions (Idea Generation)	You need ideas and information from citizens on a given issue or issues	<ul style="list-style-type: none"> IdeaScale, free at basic level: www.ideascale.com Spigit, fee for service: www.spigit.com Bubble Ideas, fee for service: http://bubbleideas.com/ Delib Dialogue App, free at basic level: www.dialogue-app.com Google Moderator, free: www.google.com/moderator/
8. Work with citizens to identify and prioritize problems that government can fix (Identify Problems)	You need ideas and information from citizens on a given issue or issues	<ul style="list-style-type: none"> SeeClickFix, free at basic level: www.seeclickfix.com OpenStreetMap, free: www.openstreetmap.org OpenLayers, free: http://openlayers.org WikiMapia, free: http://wikimapia.org Twitter, free: www.twitter.com
9. Help citizens to visualize geographic data (Mapping)	You are trying to educate and inform citizens about a particular issue or decision	<ul style="list-style-type: none"> GoogleMaps, free: www.googlemaps.com Virtual Earth, free: http://virtualearth.com WorldKit, free: http://worldkit.org/ CommunityViz, fee for service: www.communityviz.com MetroQuest, fee for service: www.metroquest.com
10. Help citizens to balance budget and revenue options (Identify Priorities)	You are trying to educate and inform citizens about a particular issue or decision	<ul style="list-style-type: none"> Budget Simulator, fee for service: www.budgetsimulator.com Budget Allocator, fee for service: www.budgetallocator.com Demos-Budget, fee for service: www.demos-budget.eu

Using Wikis in Government:

A Guide for Public Managers



Ines Mergel
Syracuse University

Best Practices for Wiki Administrators

1. **Start with a seeding phase:** In the early phases of a Wiki, it is important to generate content and support the editing process. Make it easy for people to get into online publishing: Encourage them to provide initial content that they think might be of value to the community, but have not widely shared so far.
2. **Don't write about transitory matters:** Unless the topic warrants the magnitude of an article, people should let the content grow and emerge as they find necessary. Introduce a "gardening" principle to keep content clean and on topic, merge topics if necessary, and constantly stay in contact with contributors to help them understand the established writing principles.
3. **Keep information alive:** Another way to think about content is to create information that is constantly updated, so that users want to contribute whenever new ideas arise, ideas that might be extending the existing norms or trains of thought. Instead of working toward a final document—in an encyclopedic style—the document can be supported by source material instead of replicating material. Ongoing conversations and knowledge production can be organized "rolling docs" and create what is called by Chris Rasmussen "living intelligence".⁷ Rolling documents are constantly in a beta status and are collectively improved over time.
4. **Training, training, training:** Training is essential to understand how technology works in general. Never believe that users are as tech-savvy as it may seem. There is a great deal of variety in online read-write literacy, and a hesitation to share knowledge online (loss of control). "I don't think people really know just how much they are responsible for once they become the owners of that entire process." Top management buy-in results in bottom-up participation.
5. **Set clear community rules and enforce online professionalism and netiquette:** As with every technology or innovation that is introduced to an agency, it is necessary to set standards for the appropriate and accepted use for a Wiki. Topics such as appropriate language, conduct, and defamations must be set in stone. Rules for an appropriate online discussion culture need to be addressed, and respect for contradicting and opposing opinions need to be made explicit. Moreover, think about "what ifs:" What if contributors fail to comply with the rules of the online community? Feel free to take action and remove "trolls," defamation, and inappropriate content to keep the value of the content and the overall site as high as possible.
6. **Accountability is more important than anonymity in the public sector:** On public Wikis, it is especially important to honor the principles of accountability. Contributors should sign in with a password and contact information. For internal Wikis, decide about the publishing format and make content available in an attributable manner, so that content and knowledge is connected to people. Reliability and accountability can be increased through discussions that add different perspectives, theories, and arguments. To accomplish this, apply a discussion section to encourage users to share their thoughts and justify why they made changes to existing content. This will increase the acceptance and overall accountability of the site. Content should be clearly described as non-authoritative. Wiki content should not be designed as final products, but should be seen as discussion documents that portray the overall process through which contributors arrived at decisions or knowledge. The discussion document can be seen as part of the content creation process and as a deliberative element of the overall process.

⁷ For more details watch the "Living Intelligence" video produced by Chris Rasmussen. <http://www.businessofgovernment.org>

Best Practices in Creating and Maintaining Wikis

The following best practices are based on the lessons learned by Wiki administrators and public managers reported in the nine case studies.

Best Practices for Public Managers

1. **Allow your own organization enough lead time to use a Wiki:** The organization needs to understand changes in the collaborative process, know what is needed to support the collaborative culture, understand the technology, and set up an appropriate support context (reference group, editorial team, neutral dispute coordinators, gardeners, etc.).
2. **Understand your audience(s):** Look at your audience and understand existing dynamics and responses to new challenges. What kind of knowledge is needed to address the dynamic and complex environment of your agency? How does your agency prefer to interact with citizens?
3. **Make a conscious decision about acceptable content and behavior on your Wiki:** Do not allow copy and paste of already existing internal documents that are located somewhere on the intranet or are publicly available on the web. Instead, link to locations, people, or content and focus only on innovative and new content creation on the Wiki. As result, content will not be replicated, and contributors or readers will come back for only unique content. Post your acceptable use strategy and policy prominently on the Wiki—repeat as often as necessary.
4. **Resolve disputes about content:** Forming a panel of knowledgeable and neutral parties to review content-related disputes helps to neutralize discrepancies about the content in an acceptable way. Following a clear, well-formulated strategy that is transparent to the contributors helps them understand how the conflict is resolved, encouraging them to keep up their great contributions.
5. **Formal ways of collaboration trump informal ways:** Formal ways of collaboration, for example at conferences, are long established. In addition, people tend to trust face-to-face networking with key people to talk about necessary activities. It is therefore difficult to change to informal ways of collaborating on a Wiki. A way to remedy this is to manage people and content by "walking around"—make sure that users don't think that their content disappears into a black box, but actively engage them in periodic face-to-face conversations to help increase trust in the process and show top management support for this form of collaboration.
6. **Let people pick their area of expertise:** People will be most likely to participate on Wiki pages that contain topics on which they either have an explicit expertise or on which they believe they can make a contribution. In order to support this natural tendency, move publication responsibilities as well as information management, creation, and knowledge sharing onto the actual knowledge users and experts. Provide additional incentives, such as SWAG ("stuff we all get"), recognition in employee evaluations, etc., to honor contributions and constant improvements.
7. **Knowledge moves with people:** People move on to other jobs before they can share all the information they have acquired and haven't yet downloaded onto information-sharing instruments such as Wikis. There are several ways to remove the information-sharing barrier. Make knowledge sharing a daily routine instead of a one-time download activity. Implement knowledge stewards and "gardeners" who help employees learn how to formalize their knowledge on a Wiki, and support them by fitting it into the organizational knowledge base.



Guidelines for Secure Use of Social Media by Federal Departments and Agencies

**Information Security and Identity Management Committee (ISIMC)
Network and Infrastructure Security Subcommittee (NISSC)
Web 2.0 Security Working Group (W20SWG)**

Version 1.0

September 2009

This document is publicly releasable

TABLE OF CONTENTS

INTENDED AUDIENCE	3
REVISION HISTORY	4
ACKNOWLEDGEMENTS	5
EXECUTIVE SUMMARY	6
RISKS	6
RISK MITIGATION	6
INTRODUCTION	7
USE OF SOCIAL MEDIA WITHIN THE FEDERAL GOVERNMENT	7
THE THREAT	9
SPEAR PHISHING	9
SOCIAL ENGINEERING	10
WEB APPLICATION ATTACKS	11
RECOMMENDATIONS	11
POLICY CONTROLS	12
ACQUISITION CONTROLS	13
TRAINING CONTROLS	14
NETWORK CONTROLS	15
HOST CONTROLS	16
CONCLUSION	16
WORKS CITED	18

Executive Summary

The use of social media for federal services and interactions is growing tremendously, supported by initiatives from the administration, directives from government leaders, and demands from the public. This situation presents both opportunity and risk. Guidelines and recommendations for using social media technologies in a manner that minimizes the risk are analyzed and presented in this document.

The decision to embrace social media technology is a risk-based decision, not a technology-based decision. It must be made based on a strong business case, supported at the appropriate level for each department or agency, considering its mission space, threats, technical capabilities, and potential benefits. The goal of the IT organization should not be to say "No" to social media websites and block them completely, but to say "Yes, following security guidance," with effective and appropriate information assurance security and privacy controls. The decision to authorize access to social media websites is a business decision, and comes from a risk management process made by the management team with inputs from all players, including the CIO, CISO, Office of General Counsel(OGC), privacy official and the mission owner[1]. The use of social media and the inherent cybersecurity concerns form a complex topic that introduces additional vulnerabilities, targeted by an advanced threat, requiring updated sets of controls.

Risks

Federal Government information systems are targeted by persistent, pervasive, aggressive threats. In order to defend against rapidly evolving social media threats, departments and agencies should include a multi-layered approach in a risk management program, including risks to the individual, risks to the department or agency, and risks to the federal infrastructure[1]. A defense-in-depth approach should be considered in evaluating the top three most likely threats to federal employees, infrastructure, and information. Social media technologies such as Wikis, Blogs, and social networks are vulnerable to the following methods/techniques of cyber attacks: Spear phishing, Social Engineering, and Web Application Attacks.

Risk Mitigation

This document recommends mitigating the social media risks through a series of guidelines and recommendations to assist federal departments and agencies in developing a strategy to securely enable the use of social media. These include recommendations for the creation of a government-wide policy for social media, addressing policy controls, acquisition controls, training controls, and host and network controls. Policies should not be based on specific technology, as technology changes rapidly. Rather, policies should be created to focus on user behavior, both personal and professional, and to address information confidentiality, integrity, and availability when accessing data or distributing government information. Procedures should be created and updated frequently to address the rapid changes in specific technologies. For example, acquisition controls are particularly critical when dealing with social media and other emerging technologies, because so many of them are outsourced and exist in a cloud computing environment. Additional security controls must be considered when using an externally hosted information system, including additional monitoring and configuration controls specific to federal information systems. Augmented training requirements must also be considered for federal employees using social media, due to additional attack vectors, additional security concerns, and updated policies and procedures to implement these recommended controls.

Finally, a series of technical host and network controls is recommended, from standardizing the desktop image to securing the Internet connection through a Trusted Internet Connection (TIC).

Introduction

On January 21, 2009, President Barack Obama signed a memorandum for Transparency and Open Government[2]. The Federal Government has responded with several initiatives which utilize collaborative social media technologies to engage with the public. The Federal CIO, Vivek Kundra, has stated Web 2.0 technologies are essential to "tap into the vast amounts of knowledge ... in communities across the country"[3]. Mr. Kundra has also developed a five-point plan to enable the administration's agenda: (1) Open and transparent government; (2) Lowering the cost of government; (3) Cybersecurity; (4) Participatory democracy; and (5) Innovation[4].

Cybersecurity was labeled as "crucial" for success by Mr. Kundra. To that end, this document proposes guidelines for the secure use of social media technologies within the Federal Government and provides recommendations for the creation of a government-wide policy for social media. This may require the re-education of senior management officials, as barriers are often perceived to be technology issues rather than communications, policy, strategy, or management issues. The senior technology official at each federal agency should develop a social media communications strategy, with the support of their communication office, that accurately addresses the guidelines in this document in conjunction with government-wide policy[5].

Finally, the decision for a Federal department or agency to engage with social media must be a risk-based decision making process, made using strong business justifications that identify mission requirements and drive toward an expected outcome through social media use[1]. The decision to engage or not to engage in social media use should not be made by the IT department alone, rather it should come from a risk management process made by the management team with inputs from all players, including the CIO, CISO, Office of General Counsel(OGC), Office of Public Affairs (OPA), Privacy official and the mission owner[1]. This document will outline the use cases for social media in the federal space, some of threats within this space, and some compensating controls to reduce these threats. All these should be considered as inputs to the risk management process.

Use of Social Media within the Federal Government

The use of social media technologies within the Federal Government quickly becomes a complex topic, with varying interpretations and perspectives. Researchers Dr. Mark Drapeau and Dr. Linton Wells at the National Defense University (NDU) define social media as social software, "applications that inherently connect people and information in spontaneous, interactive ways." They have articulated four specific use cases of social media within the Federal Government. These four use cases, depicted in Figure 1, include Inward Sharing, Outward Sharing, Inbound Sharing, and Outbound Sharing. While related, each use case has different threats and requires different information security controls to mitigate those threats[6].

Inward Sharing is the sharing of internal organizational documents through internal collaboration sites such as SharePoint portals and internal wikis. As this is government information hosted on government or government-contracted information systems, it falls well within the definition of a

federal information system under FISMA[7]. Inward Sharing has quite a bit of guidance addressing system security, as shown in Figure 1[6].

Outward Sharing, also known as inter-institutional sharing, enables Federal Government information to be shared with external groups, such as state and local governments, law enforcement, large corporations, and individuals. For example, agencies may use social media to communicate with the public during a time of crisis. Other examples of Outward Sharing include public websites used in a private function to facilitate the information sharing role. These include GovLoop, an externally hosted social network catering to US Government employees and contractors, STAR-TIDES, a knowledge sharing research project for complex operations, and National Institute for Urban Search and Rescue, Readiness, Response, Resilience, and Recovery (NIUSR5) using LinkedIn to connect with members and share information[6].

Inbound Sharing, also known as "crowdsourcing," is similar to conducting a large online collaborative poll. Change.gov exemplifies inbound sharing where the "Open for Questions" forum allowed over 100,000 people to participate in a government-sponsored online meeting and submit over 75,000 questions ranging from the economy, to health care, to national security[6].

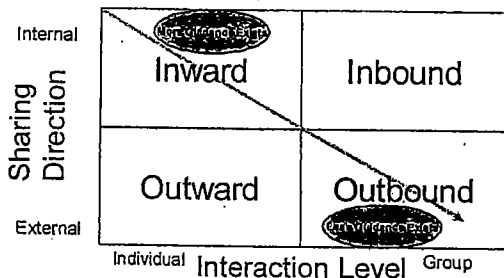


Figure 1: Four functions of social software in government and the amount of guidance [1]

Finally, Outbound Sharing is federal engagement on public commercial social media websites. The guidelines presented in this document are primarily applicable to Outbound Sharing, though they can be applied to all four use cases. For example, the authors of the NDU document cite the example of Colleen Graffy, formerly the Deputy Assistant Secretary of State for Public Diplomacy, who used Twitter to connect with foreign media before her visits to their respective countries. This gave foreign media outlets a perspective into her personality before her arrival, called "Ambient Awareness," and provided a human aspect to Ms. Graffy's official role. Ultimately she enabled more comfortable communications during her trip, and received more favorable reviews by foreign media[6].

The use of social media and the subsequent cybersecurity concerns form a complex topic that involves, not only familiar threats, but also introduces additional vulnerabilities, targeted by an advanced threat, requiring updated sets of controls. There currently exists a robust set of Computer Security laws, policies, and guidance for federal information systems from NIST, DOD, OMB, GAO, and DHS[8]. Most of this guidance addresses federal information systems, which applies to internal information systems used for inward sharing. As federal agencies engage in external sharing with larger groups, the use case shifts toward outbound sharing on non-federal information systems, as demonstrated in Figure 1. Less federal guidance exists for inbound, outward, and outbound sharing use cases, and the guidance that does exist is relatively recent. For example, the US Air Force New Media Guide, published in 2009[9], provides guidance to address these new use cases for the Federal Government.

The Threat

Federal Government information systems are targeted by persistent, pervasive, aggressive threats. This is well known and documented, as stated in May of 2009 by Margaret Graves, Acting CIO for the Department of Homeland Security.

We have now learned first-hand about this growing category of threats that directly target the Federal Government, our systems, and our information. We have also witnessed how these threats have become more persistent, more pervasive, and even more aggressive than we imagined. These actors appear to be highly-motivated and well-resourced, and it will take all of our collective efforts to keep them out of our networks[10].

As the Federal Government begins to utilize public social media websites, these advanced persistent threats may target their efforts against these websites. These attackers may use social media to collect information and launch attacks against federal information systems. By improving cybersecurity controls around current information systems, attackers are likely to target less secure information systems to reach their targets. The rapid development of Web 2.0 technologies makes it difficult to keep up with emerging capabilities and uses[6]. Security technologies should defend against new attacks, but by the time the Federal Government has caught up to the technology with policies and protection mechanisms, the technology may be outdated or surpassed by the next new development. In order to defend against rapidly evolving social media threats, the Federal Government should include a multi-layered approach to social media threats in a risk management program, including risks to the individual, risks to the department or agency, and risks to the federal infrastructure[1]. A defense-in-depth approach should be considered in evaluating the top three most likely threats to federal employees, infrastructure, and information. Social media technologies such as Wikis, Blogs, and social networks are vulnerable to the following methods/techniques of cyber attacks: Spear phishing, Social Engineering, and Web Application Attacks..

Spear Phishing

Spear Phishing is an attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link[11]. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network, but often it is easier to look up the target on a social media network. In April 2009, the Federal Bureau of Investigation released a Headline Alert specifically citing social networking sites as a mechanism for attackers to gather information on their targets by harvesting information from publicly accessible networks and using the information as an attack vector[12].

As security tools become more sophisticated, so do attackers[13]. As departments improve their security capabilities, including departmental Security Operations Center (SOC) management and improved monitoring capabilities, attackers may shift to more advanced mechanisms to target specific users. For example, spear phishing a high-value individual, also known as "Whaling," can use a customized infected document with specific information containing a unique malicious payload, making it more difficult for anti-virus companies to detect its unique signature. Quoting

Patrick Runald at the security firm F-Secure, "If you wanted to attack the CDC during the swine flu outbreak, what better way than to send something that looks like it's an internal document?" These targeted attacks seem to be replacing previous attack techniques[14].

Finally, spear phishers utilize social media as an alternative way to send phishing messages, as the social media platform bypasses traditional email security controls. Security teams have already observed multiple social media websites used as a propagation mechanism to trick users to open a document or click a link[15]. Sometimes these attacks will use URL shorteners to obscure the actual website name. The Federal Government should consider creating its own URL shortener, with appropriate logging and security, for federal use on social media websites.

Social Engineering

The second concern regarding social media use by federal employees is Social Engineering, which relies on exploiting the human element of trust[16]. The first step in any Social Engineering attack is to collect information about the attacker's target. Social networking websites can reveal a large amount of personal information, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, photos, and private information. Social media websites may share more personal information than users expect or need to keep in touch.

For example, a study by the University of Virginia cites that out of the top 150 Facebook applications, all of which are externally hosted, 90.7% of applications needed nothing more than publicly available information from members. However, all of these applications were given full access to personal information not necessary for operation, but supplied by the user granting the applications total access to their account[17].

When a federal employee joins a social media website, they may identify themselves as an employee of their department. This may happen intentionally in their profile, or unintentionally as they register with their .GOV or .MIL email address. Their self-identification creates a departmental Internet footprint, which is valuable information to our adversaries. As more federal employees self-identify on social media websites, the federal footprint on social networking will grow, creating a target-rich environment to help our adversaries target specific individuals to launch various Social Engineering and Spear Phishing attacks[18]. For example, an attacker may learn personal information about an individual and build a trust relationship by expressing interest in similar topics. Once the victim trusts the attacker, the attacker can collect more information about the user, or use their relationship to expand their influence. The attacker can expand their trust relationship to other users and friends, further gathering information and penetrating the trust of departmental personnel.

Additionally, high-profile federal employees create an even larger footprint, as they have greater name recognition, collect more friends, and often want to engage with the public. A high-profile federal employee with greater name recognition is a prime target for a social engineer to exploit the trust relationships established within that social network. In an attack similar to the "Whaling" spear phishing threat cited earlier, social engineering attacks may target high-profile individuals by relying on established trust relationships, such as close friends and colleagues. Through a compromised social media account, the attacker may pose as a friend to elicit information, action, or support[19].

Web Application Attacks

Web Applications are dynamic web pages that use scripting to provide additional functionality to the user. Using Web Applications, users may create interactive web applications. However, with additional functionalities come additional opportunities to exploit the web application. Social media websites are advanced web applications, as their use requires a high level of interaction and capabilities. This opens up social media websites to a wide range of vulnerabilities exploitable by attackers. The Open Web Application Security Project (OWASP) has published guidance to improve the level of web application security, but it is not easy to determine if a social media website is following OWASP principles and building more secure web applications[20].

Advances in web application technologies allow attackers to use new techniques against social media websites not previously possible in email. For example, emerging techniques include using custom Facebook¹ Applications to target users. Facebook applications are written by third-party developers and often have minimal security controls[21].

To illustrate this security issue, consider that a user may grant a malicious web application access to their Facebook account, which may compromise their account or download unauthorized software to their computer. This is demonstrated in Figure 2, a screenshot of the "Secret Crush" application which installs the "Zango" Spyware/Adware program[22]. Other attacks include using a Cross-Site Scripting (XSS) or similar attack to launch a javascript-based keystroke logger, capturing user keystrokes, including account usernames and passwords. Proof of concept code demonstrated this attack vector during a 2006 MySpace phishing attack that compromised 34,000 usernames and passwords[23]. Social media as an attack platform is an active area of cybersecurity research; attackers are limited only by their creativity to embrace flexible Web 2.0 technology. New attacks are emerging on a regular basis, as was demonstrated at the 2009 ShmooCon security convention in Washington, DC[24].

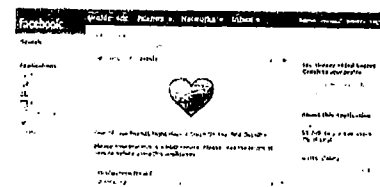


Figure 2: Secret Crush application in Facebook [22]

Finally, while a hijacked personal social media account may be annoying and personally costly or embarrassing, a hijacked account of a federal user or a federal account may have more serious implications. Unofficial posts, tweets or messages may be seen by the public as official messages, or may be used to spread malware by encouraging users to click links or download unwanted applications.

Recommendations

The following are a series of strategies and recommendations for federal departments, agencies, and policy makers to minimize risk. These solutions may be considered compensating controls in a risk management equation to enable more secure use of social media technology in a Federal Government environment. Selection of these various controls should be made specific to each

¹ Note: The Federal CIO Council does not endorse the use or imply preference for any vendor commercial products or services mentioned in this document.

agency, as each has different missions, technologies, and threats. These recommendations include both non-technical and technical security controls, and can be divided into five broad categories. Non-technical security controls include policy controls, acquisition controls, and specialized training. Technical security controls include network and host controls. The lists below are not exhaustive; other compensating controls may be considered.

Policy Controls

Social media presents a new set of tools for interactive dialog. However, users may make themselves vulnerable by trusting circles of friends and colleagues and disclosing personal facts more readily. Additionally the same phishing, social-engineering, and Web 1.0 threats (worms, trojans, etc.) may be used to exploit a friend's trust.

The safe use of social media is fundamentally a behavioral issue, not a technology issue. Policy addressing behavior associated with protecting data would likely cover current social media technologies as well as future technologies. Policies for Web 2.0 technologies, blogs, wikis, social media sites, mash-ups, cloud computing, Web 3.0, outsourced e-mail, and other new technologies will remain extensible and applicable. A policy specific to Web 2.0 or social media might be too narrowly focused; rather, procedures should be used to address the "how" question to help mitigate specific risks and provide specific solutions. The risk of using social media tools should be addressed by policies and procedures focusing on information confidentiality, integrity and availability, and user behavior, both personal and professional, when accessing data or distributing information. Federal agencies should follow the guidelines below.

- The senior technology official at each federal agency should develop a social media communications strategy, with the support of their communication office, that accurately addresses the guidelines in this document in conjunction with government-wide policy[5].
- Follow NIST Special Publication 800-39 risk management principles[25].
- Follow NIST Special Publication 800-53R3 controls, especially those for external information systems (AC-20)[26].
- Follow NIST FIPS Publication 199 to categorize information posted on social media websites and guide application of SP800-53R3 and SP800-60. For example, data posted to the public, the security categorization should be NA for Confidentiality (all public information) and no greater than LOW impact for Integrity and Availability[27].
- Follow the NIST Special Publication 800-60 categorization of the information based on the mission-based information type and intended use of the new technology[28]. Social media websites may be used for different purposes, such as outreach to the public, communication among a community of interest, or collaboration within a select group of individuals. Each scenario calls for different risk management scenarios.
- Update current policies for privacy and security in accordance with recommendations adopted from this document, including technical controls and user training.
- Update current policies for content filtering and monitoring to address functional areas of system administration and user behavior, including limiting specific activities or traffic disallowed, such as the addition of third party applications.
- Update current Acceptable Use Policies (AUP) to cover user behavior for new media technologies. User behavior includes personal use of government equipment and professional use of internal facing, public facing, and external resources. A complete AUP should address a wide array of issues, including password reuse, department

representation, commitments on behalf of Government, and security recommendations from this document.

- Update federal-level policy in accordance with this guidance as applicable.

Acquisition Controls

When Federal agencies use hosted information systems, such as social media websites, they must have some level of risk management, mitigation, and acceptance of residual risk. Most social media websites have a service subscription model that provides additional capabilities, or may be able to provide federal agencies with additional capabilities for a fee. This has already been demonstrated through modifications to Terms of Service (TOS) agreements by GSA[29]. Federal agencies should require enhanced security and privacy controls through contracted social media services, such as those listed below:

- Support stronger authentication mechanisms for federal employee and agency user profiles, including multi-factor authentication.
- Ensure social media websites consider basic security best practices, such as input validation, code security reviews, and strong cookie management. These will help to prevent common web application attacks identified in this document, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF).
- Address the federal policy issues regarding persistent cookies and their use to track users from one session to the next.
- Address federal policy issues restricting the use of comment moderation and monitoring on social media websites and accounts.
- Designate a dedicated government server or instance within the corporate social media network that provides the appropriate level of security, privacy, retention, and other security controls.
- Social media websites may identify all profiles with a ".GOV" and ".MIL" domain name email address and provide additional monitoring and stronger privacy settings. This may also involve removing certain data fields, such as the user's employer details, work location, resume, skill descriptions, or additional professional information.
- Partnerships with social media providers may allow additional visibility into federal employee accounts, and provide a mechanism to trace employee actions under a federal user account on public servers. This will assist federal incident responders when investigating social media account compromises and misuses.
- Create strong communications between Federal Security Operations Centers (SOC) and social media provider security teams. By establishing communications, roles, and responsibilities before an incident occurs, responders will be able to more rapidly resolve security incidents.
- Allow a federally operated or contracted SOC to independently monitor the security and network operations (including the NOC/SOC) of social media host contractor for contract security and incident response. This includes allowing Federal Government customers to have visibility into the social media host contractor computing environment through security and performance monitoring probes and sensors in a non-invasive manner, configuration reviews, and on-site inspections.
- Encourage social media vendors to use code validation and signing. This, in conjunction with signed code on the desktop, ensures only vetted and approved code can run on the desktop from social media websites.
- Ensure that an independent third party has conducted a risk assessment, including consideration of the level of assurance and appropriate authentication requirements for

the outsourced systems or services, in accordance with applicable federal laws and standards for system authorization, Certification, and Accreditation.

- Provide an annual information technology management optimization plan for improving security, technology, operations and service.
- Review configuration and implementation plans for production hardware and software solutions to ensure the social media provider is maintaining an appropriate configuration, patch, and technology refresh level.
- Provide proper records management retention in accordance with the National Archives and Records Administration (NARA) record schedules, Freedom of Information Act (FOIA) requests, and e-discovery litigation holds.
- Ensure the service providers make Federal Government content they host accessible at any time to the government and store it in non-proprietary and editable formats.
- Ensure production hardware and software solutions use the latest software version or no lower than one previous version plus the latest relevant patches to reduce the likelihood of vulnerabilities.

Training Controls

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.

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

Network Controls

This document does not provide any endorsement of a particular vendor technology. There are numerous vendors that provide a wide array of network security technologies that contribute to a defense-in-depth security posture for securing a department's infrastructure to enable social media. It is important to recognize that no single technology or vendor will provide a complete solution. The following are network controls that may be adopted by government agencies:

- The Federal Trusted Internet Connection (TIC) program provides a series of inspection, monitoring, detection, and blocking technologies that ensure additional security and visibility to defend against a wide array of attacks, including those discussed from a social media perspective. Web filtering and deep packet inspection technologies, including intrusion detection systems (IDS) and intrusion prevention systems (IPS), web application proxies, firewalls, and monitoring under the DHS Einstein program are a sampling of TIC technologies available today. Migrating all departmental Internet traffic behind a validated TIC provides greater visibility and security controls to enable social media technologies. Connecting to the Internet without the additional security controls provided by a TIC results in an increased risk of successful exploitation through social media and other Internet technologies[30].
- A strong department Security Operations Center (SOC) and integrated Network Operations Center (NOC) provide visibility and centralized control to respond to new threats introduced through social media. Critical to a robust SOC/NOC capability is visibility throughout the enterprise, classified access for threat intelligence, and support of senior management to take action.
- Web content filtering technologies have progressed beyond just website blocking. Current technologies allow for increasingly granular control of web applications, data, and protocols, in accordance with departmental policy. Web content filtering technologies for all Internet traffic should be located in the department TIC or provided as an add-on for offices granted access to social media websites. Several vendors provide options for robust web filtering and deep packet inspection capabilities, specifically focused on safeguarding against social media attacks.
- Department infrastructures should partition its networks into a series of security Trust Zones based on the level of security assurance required. Users granted access to social media websites should access those websites from a separate Trust Zone segmented from the rest of the department. For example, investigators requiring regular anonymous access to many potentially malicious social media websites may work in a separate zone away from office users with access to only a few social media websites. This way, a compromise in one zone will not affect other zones, and reduces the overall impact to the organization[19]. Trust Zones may also provide more granular control for Internet access through an extranet. Trust Zones can be established by the business function under its respective security assurance levels, national security classification, or FIPS 199 sensitivity category. For example, it may be acceptable to use FIPS 199 categorized low system data on an external social media website for public affairs information and workforce recruitment.
- Additional new technologies are constantly emerging to address the threats of social media.
 - Capabilities such as DNS Security (DNSSEC) provide a higher level of assurance that the website a user visits is the actual website intended. This helps to reduce the likelihood of successful spear phishing attacks.

- A shift to a data-centric protection paradigm, rather than a system-centric protection paradigm, will result in more granular data control. Allowing security, privacy, authoritative location, and authoritative duration attributes to move along with the data, as tagged attributes to the data, will ensure positive identification and enforcement of data security requirements.
- Establishing a Federal Government URL shortener with appropriate security and logging controls for use by federal employees and agencies on social media websites. This will mitigate the risk of shortened URLs used in phishing attacks.

Host Controls

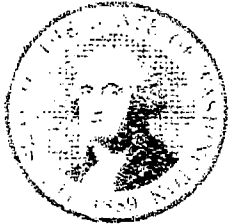
Just as important to securing the network is securing the host. Many of these endpoint protection controls are required under various FISMA, NIST, and OMB guidelines, but also provide protections specifically safeguarding against social media attacks. In addition, new technologies for host security are emerging, augmenting the growing list of options below, available for selection by a Federal Government security team.

- The establishment of a hardened Common Operating Environment (COE) will ensure consistent and comprehensive host configuration and hardening policies across the Federal Government. Hosts may be configured using the Federal Desktop Core Configuration (FDCC), and validated through a Security Content Automation Protocol (SCAP) compatible scanner.
- Stronger authentication enables greater assurance as to a user's identity, and is critical to preventing unauthorized access of federal information systems by external attackers. Two-factor authentication, such as the HSPD-12 card and PIN, provides a greater level of assurance when accessing federal information systems and workstations. Two-factor authentication reduces the likelihood an attacker will gain unauthorized access to an information system through a username and password.
- Federal agencies should ensure they have strong patching for operating system and application vulnerabilities, and that updating anti-virus signature files and system logging is enabled to report to the SOC on workstations in real time.
- The use of desktop virtualization technologies will allow users to view potentially malicious websites in a virtualized "sandbox," which safeguards the rest of the host operating system against compromise attacks against the OS. This allows the secure browsing of any potentially malicious Internet websites and can be routed through an anonymization service to provide anonymous browsing capabilities.
- Upgrade to the latest browser for users approved for social media usage. Newer browsers have additional anti-phishing technologies designed to protect against the attacks commonly used on social media websites.
- Increase the use of signed code or white listing on host workstation environments. Signed code has a higher level of assurance that it came from the approved vendor. White listing ensures only approved applications can run on the workstation. Restricting the installation of unsigned or unapproved code prevents rogue code from running on government workstations, preventing malicious code attacks.

Conclusion

The decision to engage with social media technology is a risk-based decision, not a technology-based decision, and must be made by the mission owners with input from all stakeholders, including security. The decision for a Federal department or agency to engage with social media

must be a risk-based decision making process, made using strong business justifications that identify mission requirements and drive toward an expected outcome through social media use[1]. The decision to engage or not to engage in social media use should not be made by the IT department alone, rather it should come from a risk management process made by the management team with inputs from all players, including the CIO, CISO, OGC, OPA, Privacy official and the mission owner[1]. This decision can only be made with a full understanding of the threats, risks, and mission needs. The goal of an agency's information security organization should be to securely enable the resources necessary to achieve mission objectives. This document recommends the creation of a government-wide policy based on the risks and mitigating controls presented, to provide appropriate guidance for the secure use of social media by federal departments and agencies.



STATE OF WASHINGTON

GUIDELINES AND BEST PRACTICES FOR SOCIAL MEDIA USE IN WASHINGTON STATE

OFFICE OF THE GOVERNOR IN COORDINATION WITH

MULTIPLE STATE AGENCIES AND CONTRIBUTORS

OFFICE OF THE GOVERNOR

NOVEMBER 2010

To accommodate persons with disabilities, this document is available in alternative formats and can be obtained by contacting the Office of the Governor at 360-902-4111.

VISIT OUR WEBSITE AT WWW.GOVERNOR.WA.GOV

Table of Contents

1. Introduction.....	4
Attribution.....	4
2. Purpose.....	4
3. Definitions.....	4
4. Applicability.....	5
5. Implementation.....	5
How and when to use social media sites.....	5
Create an agency social media policy.....	6
Create a process in your agency to handle internal requests to set-up social media.....	6
Authorize requests.....	6
Essential elements.....	7
6. Privacy.....	7
7. Acceptable Use.....	8
Employment Considerations.....	8
Pre-Employment.....	8
Post-Employment.....	10
Personal responsibility.....	10
Professional use.....	11
8. Terms of Service.....	12
9. Manage content legally.....	13
10. Security.....	13
Use best practices to mitigate security risks.....	14
11. Records Retention.....	14
12. References.....	15
Appendix A: Build a strong social media foundation.....	17
Appendix B: User best practices.....	18
Appendix C: Tips for social media tools.....	20

1. Introduction

The Office of the Governor and numerous state agency representatives contributed to these guidelines to assist agencies currently using social media and to encourage social media use to engage Washington state citizens. Given the evolving nature of social media, agency guidelines and policies related to social media should be reviewed and updated periodically as technologies or law develop. Staff should be trained accordingly.

Attribution

These guidelines are based on the shared experiences of other states and other state agencies, industry best practices and social media research. See [References](#).

2. Purpose

Social media offers Washington state government the opportunity to interact with the public and employees in new, exciting ways that facilitate transparency, interactivity and collaboration. These tools engage populations differently than traditional media and enhance existing communication strategies.

The Office of the Governor encourages the use of social media to advance the goals of the state and the missions of its agencies. The decision to use social media technologies is a business decision, not a technology-based decision. It is incumbent upon each agency to weight its mission, objectives, capabilities, risks and potential benefits when considering use of specific social media tools.

The purpose of this document is to provide guidelines for social media use in Washington state. State agencies may use these guidelines as a component of agency policy and procedure development. *These guidelines will evolve as new technologies and social networking tools emerge.*

3. Definitions

For purposes of these guidelines, the following definitions apply:

Comment: A response to an article or social media content submitted by a commenter.

Social networking or social media: Interaction with external websites or services based on participant contributions to the content. Types of social media include blogs, micro blogs, social and professional networks, video or photo sharing, and social bookmarking. Examples of social media sites are *YouTube, Facebook, Flickr, Twitter, WordPress, MySpace, RSS, Second Life, LinkedIn, Delicious*, etc.

Terms of Service or Terms of Use are often used interchangeably to refer to the terms that govern the use of a given website. For purposes of consistency, we use Terms of Service when referencing third-party social media application providers' terms.

4. Applicability

These guidelines are applicable to state employees or contractors who create or contribute to social networks, blogs, wikis, or any other kind of social media both on and off the wa.gov domain for work purposes.

5. Implementation

Agencies should consider how to establish and maintain approved social media presences.

How and when to use social media sites

Washington state agencies should use social media to enhance communications with the public and stakeholder organizations in support of agency goals and objectives. Social media facilitates further discussion of state issues, operations and services by providing the public and state employees with an opportunity to participate using the Internet. Consider the following when implementing a new social media tool (this is not a comprehensive list):

- Develop good principles of communication planning
 - What communications goals or objectives are you seeking to achieve?
 - Who are your audiences? Do they use these tools?
 - Which tool best achieves your goals?
 - How will you manage public records retention and public disclosure requirements?
 - How does your agency feel about social media?
 - Will you be distributing any sensitive, confidential or personal information?
 - Is the information accessible to agency customers? Consider [Section 508](#) of the federal Rehabilitation Act when you select a social media tool.
- Consider agency participation on social media websites. Will participation:
 - Create a reputational risk to personnel, the agency or the state?
 - Affect employee productivity?
 - Affect network bandwidth requirements?
 - Create security risks?
 - Create an access issue if your agency employees cannot access social media websites?
- Determine your level of participation in social media networks
 - Will you engage only in defensive tactics (responding to comments posted online, etc.)?
 - Will you consistently monitor your social media reputation?
 - How will you respond?
 - Where will you draw the line on responding?
 - Who will be authorized to respond?
 - Will you respond to comments?
 - Will you respond only to original content?
- Establish a social media presence (e.g., blog, *FaceBook* page, video, *Twitter*)
 - Who will update these pages?
 - Are you prepared to provide regular content?
 - Are you prepared for the interactivity social media requires (e.g. criticism, increased constituent contact, public records requests via social media?)

- Who will monitor comments?
- What's the approval process for using a social media tool in your organization?

Learn more about creating a good foundation for social media in your agency. [See Appendix A.](#)

Create an agency social media policy

Create a broad social media or tool-specific social media policy by using your agency's existing process for policy development and engage staff who include:

- Public affairs or communications team, including the communications director
- Information technology
- Risk management
- Public disclosure and records retention
- Contracts administration
- Assistant attorney general

Don't recreate the wheel! Use existing policies (see [References](#)) to build your policy.

Create a process in your agency to handle internal requests to set-up social media

Here are elements that should be included in a request to use social media:

- The proposed social networking platform and tools it seeks to use.
- A business case for using the new social media tool—audience, purpose, interactivity policy, etc.
- Authorized users and procedures for use. Social media tools should be administered by the state agency public affairs team or designee. Designees can be any department employee designated by the requesting department head that has a complete understanding of these guidelines, relevant agency policies and has appropriate content and technical experience. Consider writing guidelines for authorized users of social media tools.
- A risk assessment. The risk assessment should include, at a minimum, the analysis of the risks (including risk mitigation strategies) involved in providing users access to social media websites including:
 - Employee productivity
 - Network bandwidth requirements and impacts
 - Reputational risk to personnel, the agency and the state
 - Potential avenue for exposure or leakage of sensitive or protected information such as copyrighted material, intellectual property, personally identifying information, etc.
 - Potential avenue for malware introduction into the organization's IT environment

Authorize requests

Requests should be approved by a collaborative social media advisory composed of these representatives of the agency:

- Deputy director
- Public affairs or communications team, including the communications director
- Information technology director

- Risk management officer
- Public disclosure and records retention officer
- Contracts administration officer
- Assistant attorney general

This committee should meet as needed to review agency requests for social media use. See an example of a social media advisory committee.

Essential elements

Once implemented (and where possible), state agency social media sites should consider including the following elements:

- An introductory statement that specifies the purpose and scope of the social network site.
- Links to the official state agency Internet site for forms, documents and other information.
- Policies for the use of the tool including:
 - **Comment and moderation-** To allow moderation of comments without running afoul of the First Amendment, consider creating a comment and moderation policy. See examples in the References section.
 - **Distribution-** Use language such as “Anything you read here may be distributed or reproduced. We ask that you attribute the information to <state agency blog>, as appropriate. Information from external news sources or websites that you access from this site may be subject to copyright and licensing restrictions (or laws), and you should check directly with sources before distributing such content.”
 - **Linking-** Use language such as “When you select a link to an outside website, you are leaving the <state agency social media tool> and are subject to the privacy and security policies of the owners/sponsors of that site. The state agency is not responsible for transmissions users receive from external websites.”
 - **Disclaimer of endorsement-** Whether ads appear on social media websites may be beyond an agency’s control. Accordingly, a statement along the following lines should be included: “Reference to any specific commercial products, processes or services, or the use of any trade, firm or corporation name does not constitute endorsement or recommendation by the Washington state, the state agency or its employees.”

6. Privacy

State agencies should review the privacy policy of social media sites to determine if it is consistent with federal and state privacy obligations. In addition, review should be made of policy on data stewardship. Attention should be paid to the privacy policy to determine implications on end users, including but not limited to whether the policy:

- Permits companies to track users of government websites for advertising purposes.
- Allows access/disclosure of user information, including usage history.
- Allows for selling user-provided information.
- Allows for recording information about site usage.

- Allows for opting out of any data collection processes.
- States where the data will be physically maintained.

If the agency uses persistent cookies,¹ on its own site, the agency should review that decision with its assistant attorney general to assure that agency behavior is consistent with its privacy policy.

7. Acceptable Use

State agencies, departments and employees using social media are generally subject to all appropriate agency and state policies and standards, including but not limited to:

- Applicable state, federal, and local laws, regulations and policies, including all information technology security policies
- Agency and statewide acceptable use policies
- Agency and statewide ethics laws, rules and policies
- Agency linking policies (e.g. linking to external websites from an agency website and establishing a link from an external website to an agency website)
- Public Records Act and e-discovery laws and policies (requiring content to be managed, stored and retrieved)
- Applicable records-retention laws and schedules
- Applicable policies, procedures, standards or guidelines of the Information Services Board Web Presentation and Accessibility Standards

Any exceptions must be approved by the agency director and are subject to review by the agency chief technology/information officer.

Employment Considerations

Pre-Employment

As employers, agencies should take account of the following points/concerns.

- Establish a written policy before using social media resources in hiring or recruiting. At a minimum, the policy should address the considerations below, including employment considerations and employer use of social media for human resources purposes.
- Consider the risks in depending on information gathered from social media sources in screening, conducting background checks or making hiring or other employment decisions such as promotions, transfers, or layoffs.
- Consider whether to use social media resources for pre-employment human resource purposes.
- If an employer decides to use social media as a screening tool in hiring or other employment decisions, the employer should:

¹ At this time, federal government agencies are forbidden from using persistent cookies in most cases on federal websites. Washington state has not adopted a formal position with respect to persistent cookie deployment on state websites. Third-party commercial websites are likely to have persistent cookies or other mechanisms for tracking consumer behavior.

- o Be able to identify and document the legitimate non-discriminatory reasons or bona fide occupational requirement related to the use of the screening information for hiring or other employment decisions.
- o Be skeptical of information that is discovered and investigate further if necessary.
- Be aware of generational diversity and different communication styles in the employee population as information is assessed that is deemed job-related.
- Recognize that this is a new and developing area of the law. Accordingly, it is recommended employers proceed thoughtfully and work closely with their assigned assistant attorney general.

If an agency uses social media websites to investigate backgrounds of candidates for employment or other employment decisions, such screening should apply to [choose one]:

- All candidates for employment [or]
- Candidates for employment only under the following conditions: [Specify the circumstances, for example for certain positions.]

Any use of social media for pre-employment screening will be performed based on procedures established by or through established guidelines. In reviewing information derived from social media sites, agencies:

- Will consider only information that is job-related. Some information shared on social media sites will reveal information such as religious views, marital status or other protected categories or status under the law against discrimination. This information should have no bearing on employment decisions.
- Not permit staff to “friend” candidates to gain access to non-public social media sites.

Agencies should:

- Establish a written policy governing pre-employment screening or investigations.
- Establish a list of specific sites to be checked; and not review sites on an ad hoc basis.
- Obtain a candidate’s written permission to review social media sites prior to any review and establish a policy regarding the impact if the candidate declines to consent to a review of social media sites.
- Identify appropriate human resources staff to review social media sites, filter out any information that is not job-related, and provide a summary for decision makers (staff conducting reviews should not be involved in making hiring or other employment decisions).
- Establish a procedure for independent verification of any significant results on social media sites or public websites.
- Make a record of relevant information found on social networking sites, such as by capturing a screen shot of a social networking web page, only under the following circumstances: [Specify the circumstances, for example, staff has located information believed to bear on candidates’ fitness or qualifications for a specific position].

Agencies are encouraged to consult with their assigned assistant attorney general within the [Attorney General’s Labor and Personnel Division](#) before using social media to conduct pre-employment background checks.

Post-Employment

Agencies should establish a policy on social media use before acting upon social media issues in the employment context. An agency may choose to address the use of social media in several ways, including:

- Blocking access to social media sites at work for some or all employees.
- Permitting social media to be used in the workplace for defined business purposes only.
- Permitting social media to be used in the workplace for defined business purposes and, consistent with state ethics law, for de minimis personal use.

Agency policies allowing use of social media for professional networking as a business purpose, or allowing de minimis personal use of social media, do not automatically insulate an employee from an ethics violation finding by the Executive Ethics Board. Employers are strongly encouraged to request the Executive Ethics Board to review policies that address employee use of social media, as provided in [RCW 42.52.360\(5\)](#).

Employers should consider laws, policies or legal doctrines that may be implicated in employee use of social media in and beyond the workplace, including but not limited to:

- State and federal anti-discrimination and anti-retaliation laws;
- Privacy protections and circumstances where an individual does or does not have a legitimate expectation of privacy;
- [Stored Communications Act](#) (prohibits unauthorized access of stored communications including social media posts, email and voicemail);
- State [whistleblower laws](#); and,
- Laws or agency policies related to off-duty conduct.

Employers should also be aware that any new social media policies may affect the terms or working conditions of employees. As such, some of the topics within the policy may be a mandatory subject for bargaining. It is recommended that agencies contact their assigned assistant attorney general with the [Attorney General’s Labor and Personnel Division](#) for guidance.

All supervisors and human resource professionals should be trained on the appropriate use of social media. The policy should be revisited frequently because the use of social media continues to evolve at a rapid pace.

Personal responsibility

Be thoughtful about how you present yourself in online social networks, where the lines between public and private, personal and professional are blurred.

Wherever possible, consider the following issues:

- **Confidentiality**- Employees will not post or release proprietary, confidential, sensitive or personally identifiable information or state government intellectual property on social media websites. [Learn more about Information Services Board Information Technology Security Standards.](#)

- **De minimis use-** Employees must adhere to their agency de minimis use policy and the state ethics laws governing de minimis use. If you are not certain about the criteria for de minimis use, consult your agency policies or ask an agency supervisor or human resource consultant.
- **Disclaimers-** If employees identify themselves as a state employee on a social networking site, wherever appropriate, use a disclaimer (e.g. "While I work for a state agency, anything I publish is my personal opinion and not necessarily the opinions or position of my agency or state.")
- **Personal vs. professional use-** Employees' personal social-networking sites should remain personal in nature and should not be used for work-related purposes. Employees should not use their state e-mail account or password in conjunction with a personal social networking account.
- **Use of state resources-** Employees may not use state-owned resources (computer, network, cell phone, etc.) to access social networking websites unless authorized to do so for official use. Employees must not use any state resources to access social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Please refer to [WAC 292-110-010](#).
- **Ethical obligations-** Some state ethical obligations must be followed at all times, even when employees engage in social media use in their personal capacities. For example, employees must not disclose confidential information acquired by the employee by reason of the employee's official position. See [RCW 42.52.050](#). This restriction applies regardless of whether the information is disclosed on a personal or a state social media site.

Professional use

All agency-related communication through social media outlets should remain professional in nature and should be conducted in accordance with the agency's stated communications policy, practices and expectations. Employees are expected to use good judgment and take personal and professional responsibility for any content they publish via social media. Refer to [Appendix B: User Best Practices](#) for more information.

Wherever possible, state agencies, departments and employees must consider at least the following:

- **Authorization-** Employees should not participate on social media websites or other online forums on behalf of an agency unless authorized by the agency head or the agency's communication director or designee. Users may not speak on behalf of the state unless specifically authorized by the Office of the Governor.
- **Confidentiality-** Employees will not post or release proprietary, confidential, sensitive or personally identifiable information or state government intellectual property on social media websites. These guidelines should not be interpreted to prohibit protected communications, such as attorney-client communications. However, social networking or social media would not, in general, be an appropriate forum for confidential communications. Learn more about [Information Services Board Information Technology Security Standards](#).
- **Disciplinary action-** For purposes of considering disciplinary action, agencies can treat acts or omissions occurring in the context of social media in the same manner as any other employee act or omission. Failure to abide by policies established for use of social media may result in the loss

of any social networking privileges. As with any policy, violation may also result in disciplinary action, up to and including dismissal.

- **Ethics-** Before an agency posts a website hyperlink to a social networking site, the communications director or delegate should evaluate the likelihood that the proposed website link will post political materials.²
 - In the case of non-political organizations or sites that do not have a history of political advocacy, the communications director or delegate should verify the content and establish a reporting mechanism that encourages the agency's website users to notify the agency if political materials are being posted or linked therein.
 - In the case of organizations or sites known to support or oppose candidates for public office, or to advocate for or against ballot initiatives or referenda, the communications director or delegate should establish links to or from the agency's websites if there is no political advocacy on the linked web page or if the agency holds a written agreement that the organization or site will not place political advocacy on the linked web page without notifying the agency.
- **Identify yourself clearly-** When creating social media accounts that require individual identification, authorized users speaking on behalf of the agency should identify themselves, if possible, by: 1) full name; 2) title; 3) agency; and 4) contact information, when posting or exchanging information on social media forums.
- **Privacy-** Employees should have no expectation of privacy in information stored on state computers or devices. Furthermore, there should be no expectation of privacy when employee conduct concerns the agency or its clients.
- **Permitted use-** Staff may use social networking only for approved business purposes, including professional networking, to support their agency's mission provided they follow their agency's state resource use policy. Use of social networking for personal purposes is not permitted on agency equipment.

Refer to [Appendix C](#) for social media tool tips.

8. Terms of Service

Typically a Terms of Service (TOS) is associated with the use of third-party social media tools. Each tool usually has its own unique TOS that regulates how users employ the tool. In order to avoid violations, any employee implementing social media on behalf of a state agency should consult the most current TOS and review it with the agency's assistant attorney general. If the TOS contradicts agency policy, the communication director should be made aware of it and a decision should be made about whether use of such media is appropriate.

Wherever possible, state agencies, departments and employees must consider at least the following:

² Adapted from [Washington State Department of Information Services Posting to Social Networking Sites policy](#).

- Who is authorized to open a “free” account with a third-party provider, which entails agreeing to TOS (executing a contract via “click through” agreement)
- Who will read a TOS, prior to entering such agreements, to determine whether the TOS contains:
 - Terms that are problems for the agency or that are “deal breakers”
 - Terms that are a good fit for the intended purpose
 - Provisions that require the agency to monitor use
 - Benefits of the platform that outweigh the risks
- Who will monitor provider’s site for unilateral amendments to TOS
- Who will determine how amendments will be addressed

9. Manage content legally

It is critical that agencies comply with laws governing copyright. Agencies must also respect individual privacy rights. When posting materials, agencies should:

- Obtain copyright releases for all material protected by copyright from the creators, or indemnification from the entity for which the material is to be posted.
- Obtain personality right releases or “model releases” for each image (including video) of a person who may have a potential claim to such a right, or indemnification from the entity for which the material is to be posted.

If the agency receives proper notification of possible copyright infringement, it will remove or disable access to the allegedly infringing material and terminate the accounts of repeat infringers.

Use of limited excerpts of a copyrighted work may fall within the “Fair Use” Doctrine which allows certain limited uses of such excerpts without constituting an infringement of copyright. In determining whether use in a particular case is a “fair use,” the factors considered include:

- The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- The nature of the copyrighted work;
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- The effect of the use upon the potential market for or value of the copyrighted work.

Similarly, there are limited exemptions from the requirement to obtain consent before the use of a photograph or video of a person, including where there is “insignificant, de minimis, or incidental use.” See [RCW 63.60.070](#).

10. Security

Agencies should consider how to prevent fraud or unauthorized access to social media sites. In almost every case where an attacker accesses a system without authorization, he/she does so with the intent to cause harm, including:

Mild forms of harm	More serious forms of harm
<ul style="list-style-type: none"> • Making unofficial posts, tweets or messages that will be seen by the public as official messages. • Encouraging users to either click links or download unwanted applications that the attacker has added to the site. 	<ul style="list-style-type: none"> • Accessing, compromising or disabling a state system. • Redirecting users to sites that look like a state site but are used to gather data that could be used for unauthorized purposes (i.e. <u>phishing</u>). • Using a compromised site to spread <u>malware</u>. • Acquiring confidential information about state employees or citizens (i.e. <u>social engineering</u>).

Use best practices to mitigate security risks.³

Security related to social media is fundamentally a behavioral issue, not typically a technology issue. In general, employees unwittingly providing information to third parties pose a risk to the state network. Employees need to be aware of current and emerging threats that they may face using social media website and how to avoid falling prey. If agencies participate in social networking, agencies should:

- Use a separate user IDs and password to access social networking sites.
- Never duplicate user IDs and passwords across multiple social networking sites.
- Train users about what information to share, with whom they can share it, and what not to share.
- Educate users about security awareness and risks when using social media.
- Help employees set appropriate privacy settings for social networking websites.
- Develop a social media strategy and policy that addresses security risks and mitigates them to the extent that the agency is comfortable using specific social media tools.
- Update current Acceptable Use Policies to cover user behavior for new media technologies. User behavior includes personal use of government equipment, de minimis use, and professional use of internal facing, public facing, and external resources.
- Consider disaster recovery requirements in the event that your agency hosts your own social media services. Work with your agency’s IT department to establish clear recovery time objectives.
- Regularly apply Microsoft patches.
- Review (and apply as appropriate) patches for Firefox, Adobe and Java as these softwares are common paths for security vulnerabilities.

11. Records Retention

Agencies should consider the following regarding the retention of public records of posts to social networking websites:

- The agency recognizes that all content published and received by the agency using social media in connection with the transaction of the agency’s public business are public records for the purposes of [Chapter 40.14 RCW \(Preservation and destruction of public records\)](#).

³ Adapted from [Best Practices for Social Media Usage in North Carolina](#)

- The agency remains responsible for capturing electronic copies of its public records made or received using social media, including those records made or received using third-party websites.
- The agency must establish mechanisms/procedures to capture and retain public records made or received using social media.
- Agencies should consider methods for capturing social media public records. In addition to establishing a separate agency email account for social media tools, consider using or developing applications that capture social media records. Some third-party tools include (this is not an exhaustive list):
 - [TwiInbox](#)
 - [Tweetake](#)
 - [SocialSafe](#)
 - [Cloudpreservation](#)
- The agency retains social media public records and disposes (destroys or transfers to Washington State Archives) social media public records only in accordance with records retention schedules approved by the State Records Committee under [RCW 40.14.050](#).
- This agency applies records retention schedules to social media public records consistent with the application to non-social-media public records, based on the function and content of the public record. For example, comments received via social media are retained for the same period as they would have been if they had been received by the agency via email or non-electronic means.

For additional information, please refer to the Secretary of State [Blogs, Wikis, Facebook, Twitter & Managing Public Records](#).

12. References

Federal & Private Entities

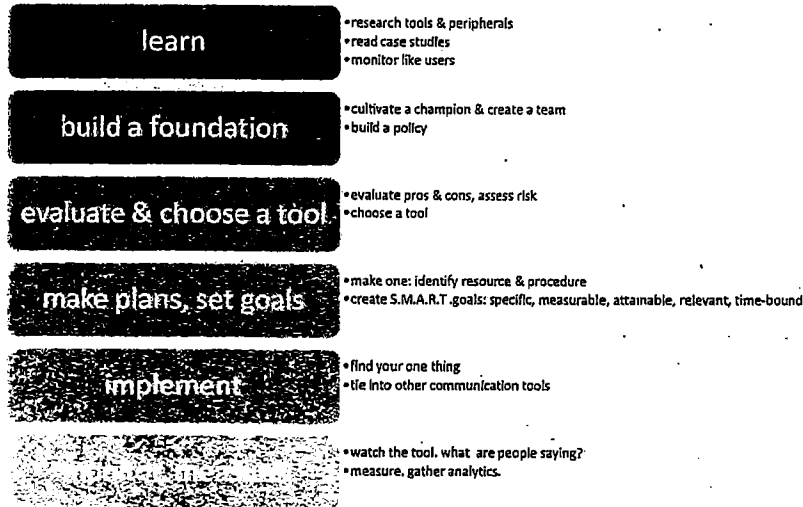
- [CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#)
- [General Services Administration Social Media Handbook](#)
- [General Services Administration Social Media Policy](#)
- [IBM Social Computing Guidelines](#)

City, State and Local

- [Best Practices for Social Media Usage in North Carolina](#)
- [City of Seattle Social Media Use Policy](#)
- [City of Seattle City Council](#)
- [Massachusetts Governor's Office Social Media Usage and Policies](#)
- [New York State Social Media Policy](#)
- [State of Oregon Social Networking Guide](#)
- [State of Utah Social Media Guidelines](#)
- [Washington State Attorney General's Office Blog Comment and Use Policy](#)
- [Washington State Department of Ecology Blog Commenting Policy](#)
- [Washington State Department of Licensing Blog Use Policy](#)

- [Washington State Department of Information Services Posting to Social Networking Sites](#)
- [Washington State Department of Transportation Comment Policy](#)
- [Washington State Labor and Industries Social Media Policy](#)
- [Washington State Secretary of State Blog Use Policy](#)
- [Washington State Secretary of State Blogs, Wikis, Facebook, Twitter & Managing Public Records](#)

Appendix A: Build a strong social media foundation



Appendix B: User best practices

Social Media is an important way for agencies to interact with the public and state employees. The Office of the Governor encourages the use of social media as it offers opportunities for outreach, information sharing and interaction. These best practices are not rules that must be followed, but general information about the culture of social media and how to be a good citizen of the social media environment.⁴

Be responsible- You are personally responsible for the material you post. Remember, you are speaking on behalf of your agency. Carefully consider content; what you publish will be widely accessible for some time and, in some cases, indefinitely. All statements must be true and not misleading.

Be honest & transparent- Your honesty – or dishonesty – will be quickly noticed in the social media environment. Use your director's name and photo only if he or she will be the one to post on the site. Otherwise, use your agency and/or division's name and logo.

Correct errors quickly- If you make a mistake, admit it. Be upfront and quickly provide the correct information. If appropriate, modify an earlier post to make it clear that you have corrected an error.

Be respectful- When disagreeing with others' opinions, keep it appropriate and polite. Do not use defamatory, libelous or damaging innuendo, to include abusive, threatening, offensive, obscene, explicit or racist language. Do not post illegal material.

Be relevant and add value- There is a lot of written content in the social media environment. The best way to get yours read is to write things that people will value. Social communication from agencies should help citizens, partners and co-workers. It should be thought-provoking and should also build a sense of community. If social communication helps people improve knowledge or skills, build their businesses, do their jobs, solve problems, or understand the state better, then social media adds value.

Stick to your area of expertise- Provide unique, individual perspectives on what is going on at your agency, and in other larger contexts. Post meaningful, respectful comments that inform, educate and engage citizens. Do not just repost press releases. Example: An environmental agency might post information they generate regarding endangered species, share information from other sources about natural resources, or comment on another source's information on carbon footprints, but they wouldn't post information about licensing foster homes.

Respect proprietary information, content and confidentiality- Always give people proper credit for their work. Make sure you have the right to use material with attribution before publishing. It is a good practice to link to others' work rather than reproducing it on your site. If posting photos or videos be sure to have all non-agency staff depicted sign a model release.

Respond quickly- When a response is appropriate, reply to comments in a timely manner. If you allow comments, be sure you have enough staff time to review the comments on a regular basis and select a person(s) who is allowed to respond on behalf of the agency. Example: "You are doing a great job

⁴ Adapted from [IBM Social Computing Guidelines](#), [State of Utah Social Media Guidelines](#) and the Washington State Bar Association Social Networking Policy.

Agency X” – does not need a response, but “You are doing a great job Agency X, how can I get involved?” – does need a response.

Be conversational- Talk to your readers like you would talk to a person on the phone. Bring in your own personality to find the voice/tone of your agency. Use plain language and avoid using government jargon or acronyms. Consider content that is open-ended and invites response. Encourage comments. Broaden the conversation by citing others who are commenting about the same topic and allowing your content to be shared or syndicated. When shortening words to save space, utilize commonly used shorthand.

Abide by social networks rules- By joining a particular social network, you agree to abide by that community’s terms of service, so review those terms carefully. Be a good citizen of the social media world and adhere to its unwritten rules of etiquette.

Follow applicable agency policies- Be sure to adhere to your agency’s applicable policies, including Social Media Policy, Internet Use Policy, IT Security Policy, etc.

Don’t forget your day job- You should make sure that your online activities do not interfere with your job or commitments to customers.

Appendix C: Tips for social media tools

Twitter

- Tweets should be less than the 140 allowed characters to allow others to re-tweet without having to remove some of your content
- Use a URL shortener/tracker to save space and count click-throughs
- Follow back those who follow you, except if they have an inappropriate photo or tweets
- Re-tweet others whose content is relevant and may be of interest to your followers
- Thank those who re-tweet your tweets with an at reply (@ reply)
- Use hash tags (#) when appropriate to make your tweets more searchable
- Respond quickly to direct messages (those that aren’t spam)

YouTube

- Have a model release for any non-agency staff in the video
- Follow all applicable copyright laws
- Use terms in the title, description and key word sections to make video more searchable
- Allow video to be embedded on other sites to spread video to the widest possible audience

Facebook

- Consider whether a profile or “like” page best meets your agency’s needs
- Be sure to keep an agency or agency director’s official state page separate from an agency director’s personal page
- Allow comments to create two-way conversation
- Post a comment policy to create a limited public forum that allows you to moderate the comments and delete inappropriate content. Consult with your agency’s assigned assistant attorney general on how to accomplish this task.
- Determine if you have the resources to respond to direct messages and who should respond

Wikipedia

- Source all your content or it will be removed by the moderators

Blog

- Be clear about who is posting each post
- Use hyperlinks to link to more information if appropriate
- Allow comments to create a two-way conversation
- Post a comment policy to create a limited public forum that allows you to moderate the comments and delete inappropriate content. Consult with your agency’s assigned assistant attorney general on how to accomplish this task.
- Post regularly



Electronic Records Management: Blogs, Wikis, Facebook, Twitter & Managing Public Records

The purpose of this advice is to provide guidance to state and local government agencies regarding the retention of public records of posts to social networking websites such as blogs, wikis, Facebook, Twitter, etc.

Agencies need to consider the following five (5) factors when managing the retention of their public records created or received through social networking sites:

1. Are the posts public records?

If the posts are made or received in connection with the transaction of the agency's public business (such as providing advice or receiving comments about the agency, its programs, core business, etc.), then they are public records for the purposes of records retention and need to be retained for their minimum retention periods.

2. Are the posts primary or secondary copies?

If the posts are simply copies of records that the agency is already retaining for the minimum retention period (such as links to publications), then the posts may be considered secondary copies and retained accordingly. Otherwise, the posts are the agency's primary record.

3. How long do the posts need to be retained?

Agencies should use the same records series for posts that they would use if the same advice was distributed as a letter or an email to everyone within the agency's jurisdiction. Agencies need to retain their primary record of posts which are public records for at least the minimum retention period listed for those records in the approved records retention schedules.

4. How will the posts be retained by the agency?

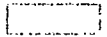
Agencies need to consider how they will retain a record in their custody and control of their posts to social networking websites. When retention of the posts themselves is outside the agency's control, the agency needs to consider what other records they will retain, such as email confirmations of each post or comment. Agencies need to consider these issues in any service contracts with vendors of social networking websites and in their configuration settings for their social networking website accounts.

5. For which types of records is this technology appropriate?

Agencies need to determine the business activities for which social networking technology is appropriate if the agency is unable to manage the creation, receipt and retention of public records documenting the public business they transact using social networking websites.

**Additional advice regarding the management of public records is available from
Washington State Archives:**

www.secstate.wa.gov/archives
recordsmanagement@secstate.wa.gov



[Home](#) » [Web Manager University](#)

TOOLBOX

[Receive updates by email](#)

[SHARE](#) [FB](#) [TW](#)

Web Manager University

Practical and affordable training for anyone who works on a federal, state, tribal, local, or territory U.S. government website.

Upcoming Events

Jul 14: [USASearch Program](#)

Jul 20: [First Fridays Product Testing](#)

Jul 21: [Monthly Forum Call](#)

Our [past new media talks](#) and [archived webinars](#) offer more great training opportunities.

[About WMU](#)

Who we are and our mission

[Schedule of Classes](#)

Online webinars, 1- and 2-day training events

[Registration & Payment](#)

Information about registering and paying for WMU events

[WMU Instructors](#)

Biographies of our world-class faculty

[New Media Talks](#)

Free seminars given by top industry professionals

[Annual Conference](#)

Web professionals meet and exchange ideas

[Previous Training](#)

Archived webinars and past New Media Talks

[Contact WMU](#)

Email or call WMU

Follow Us:



Page Updated: July 6, 2011