



The Social Media Navigator

GSA's Guide to Official Use of Social Media

April 2011

Table of Contents

Chapters:

1: Introduction – Guidance for the Official Use of Social Media	3
2: What is Social Media?	3
3: What “Official Use” Means	4
4: Considerations When Choosing a Social Media Product	5
5: Your Responsibilities	6
Get Approval First	6
Minimize Your Risk	6
Nonpublic Information	6
About Endorsements of Products, Services, or Enterprises	7
Section 508 Standards (Accessibility)	7
Practice Proper Records Management	7
Know the Laws for Information Collection	8
Plain Language	8
Meet Information Quality Standards	8
Ensure Meaningful Access by People with Limited English Proficiency.....	9
Protect Intellectual Property	9
Privacy Considerations.....	10
Cookies	10
Provide Data in a Usable Format	10
Adhere to Lobbying Rules	10
Avoid Political Activity (Hatch Act).....	11
Know When the Federal Advisory Committee Act Applies	11
Monitor What You Control	11
6: GSA Encourages and Supports Social Media.....	12
7: Social Media Use Should Be Strategic	12
8: GSA Has the Right to Monitor and Remove Comments	13
9: This Guide Will Continue to Be Reviewed	13
APPENDIX:	14
A. Requirements Checklist When Using Social Media.....	14
B. More Advice for Engaging in Online Conversations.....	15
C. Frequently Asked Questions	16
D. Guidance for Bloggers	18

E. Risks And Mitigation Strategies	22
F. How Agencies are Using Social Media	25

1: Introduction – Guidance for the Official Use of Social Media

Purpose

The Social Media Navigator is a Guide to GSA’s official use of social media, which augments the GSA Directive on Social Media Policy. The scope includes the use of social media technologies hosted outside of Federal Government servers, social media technologies hosted on internal Federal Government servers, and individual user’s responsibilities when accessing social media services in either environment in an official capacity.

1. Applicability

This Social Media Navigator is designed to guide GSA employees in their official use of social media. Employees are also highly encouraged to take GSA’s Social Media Awareness training at [GSA’s On-Line University](#).

2. Background

GSA encourages the use of appropriate social media technologies to enhance communication, collaboration, and information exchange. GSA has signed agreements with social media providers, such as Flickr, Facebook, YouTube, Vimeo and blip.tv that make it possible for GSA employees to use external social media technologies for official use while meeting current legal requirements. This Guide is not a substitute for legal guidance, so employees engaged in social media activities on behalf of GSA are encouraged to contact the Office of General Counsel (OGC) at (202) 501-2200 when specific questions arise.

2: What is Social Media?

“Social media”, also known as “Web 2.0” or “Gov 2.0” in the case of Federal Government use, are web-based, interactive tools and media, oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online. Their interactions with the information (both collectively and individually) can significantly alter the experience of subsequent users.

Social media is different from traditional media

Sites like Twitter, Facebook, YouTube, Flickr, and others are the first media that make it easy for anyone to reach large numbers of people without having great resources. Anyone can use the Internet to reach millions of people just by posting a blog, sharing a video, or posting a question on Twitter. With social media, anyone who can consume information can produce it too. On social media, information spreads not by broadcast, but through sharing. (That’s what makes it social!) That makes it an ideal platform for sharing information, starting conversations, and exchanging knowledge within and outside Government. If you

have a problem that makes you think, "I wish I could get more people involved in this discussion," social media may be for you!

Social media tools can be extremely valuable for collaboration within and across an enterprise by enabling more efficient creation, sharing, and discovery of collective knowledge. Government is constantly finding ways to use social media tools to communicate with citizens, discover their needs and ideas, deliver services more effectively, and work more efficiently across silos. To learn more about some of these, you can explore the [White House Innovations Gallery](#). Here are two things to consider when deciding whether and how to use social media to get your work done.

1. Social media is about putting information where people are looking for it.

One of the Federal Government's most important missions—especially here at GSA—is to provide citizens, customers, and partners with easy access to Government information and services. We have many ways of doing this, but the rise of social media means we have to add new tools to our arsenal. YouTube is now the second largest search engine in the world. More than 25 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month on Facebook. New Twitter users sign up at a rate of 300,000 per day. These venues aren't just where content is discovered, but where it is shared. That's why, when GSA publishes information through an article or press release, we also update our official Facebook page, <http://www.facebook.com/GSA>. It's why when we want to communicate about the technology programs we make available to Federal agencies, we get the word out through our website, but also through Twitter at <http://twitter.com/GSA ITS>. Social media is a way of making sure that our message is in the places where our citizens, customers, employees, and stakeholders regularly interact, and that it reaches interested audiences we may not even know about.

2. Social media relates directly to our mission of providing great solutions.

Because platforms like Facebook and Twitter are visually appealing, highly social, and often quite fun to use, it's easy to see them as recreational, or something that stands alongside the "real" work of GSA. There's no question that, as with any tool or resource, all supervisors have a duty to ensure that GSA's use of social media is focused and mission-oriented. When meeting those criteria, social media can be an incredibly powerful tool, precisely because it connects us directly to such a diversity of audiences and opinions. A collection of GSA's social media endeavors can be found at: <http://www.gsa.gov/socialmedia>.

3: What "Official Use" Means

There is an "official" you and a "personal" you. The "official" you is the person who represents and speaks on behalf of GSA. The "personal" you is the person who represents your own views and opinions. The difference between official use and personal use of social media is:

- **Personal Use:** You can do anything that's not illegal.

- **Official Use:** You can only do what you are authorized to do.

This Guide, the Social Media Navigator, provides guidance on the use of social media tools in an official capacity. So, let's talk about the "official" you: in other words, when you are communicating in your official capacity using social media. These types of communications may typically occur in two areas:

- Communication on GSA's official sites (e.g., our YouTube, Facebook or Twitter accounts).
- Communication on someone else's site (e.g., responding to a posting on another web site).

What "Official Capacity" Means

You know you are communicating in your official capacity when your supervisor assigns this activity as part of your official duties. Your supervisor should clearly explain the scope of the assignment and what social media tool or tools you can use. This is different from your "personal" use. The important point is that when you communicate in an official capacity you are communicating on behalf of GSA, just as if you were standing at a podium at a conference, communicating the Agency's views to everyone.

What "Personal Use" Means

Personal use means the use of social media to represent your own views and opinions. Obviously, you are certainly allowed to have personal websites, Facebook accounts, blogs and the like outside of work. However, it is important to remember that when you use your social media tools in your personal capacity, you are not speaking for GSA and it should not appear to others as though you are speaking for GSA.

4: Considerations When Choosing a Social Media Product

The choice to use a social media tool should be carefully considered. Think about the target audience and what the ultimate goal of the GSA organization is, and then choose a tool that is suitable to accomplish that goal. The decision should be made by a person with authority within the Service or Staff Office. If the desired tool is not already listed on Apps.gov as having a GSA-signed [Terms of Service Agreement](#), contract, or other agreement authorizing its use, then work with the appropriate contracting office, the Office of General Counsel, and/or the Center for New Media and Citizen Engagement to obtain the appropriate clearance for GSA to use the specific social media tool. Use caution to avoid accepting the standard "click-through" User Agreement on most websites as they contain provisions that the Federal Government cannot legally accept. Office of Management and Budget (OMB) [OMB Memorandum M-05-04](#) advises when information must be on a ".gov", ".mil", or "Fed.us" website. For examples of how others at GSA are using social media go to www.gsa.gov/socialmedia.

5: Your Responsibilities

Get Approval First

After you have the approval of your supervisor, it is your responsibility to gain approval from whoever in your organization has executive oversight or responsibility for the subject matter that will be the main focus of your social media effort. Please notify the Office of Communications and Marketing at socialmedia@gsa.gov, so that they can maintain an updated list of GSA's social media presences. Please also notify the Office of Communications and Marketing about your effort if you plan to write about content that may have a high public profile or attract media attention.

Minimize Your Risk

Social media tools and technologies, such as Facebook, YouTube and Twitter, offer GSA employees powerful channels to deliver relevant and targeted marketing and outreach messages, often facilitated through trusted sources, when, where, and how users want information. 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. To ensure that GSA's use of social media is both safe and effective, please thoroughly read Appendix E, Risks and Mitigation Strategies, which provides recommendations and a due diligence checklist to protect the GSA network by mitigating security risks posed by social media tools.

Nonpublic Information

Various laws and regulations may prohibit the disclosure of certain information. Provisions in the Privacy Act, Procurement Integrity Act, Freedom of Information Act (FOIA), National Defense Authorization Act of 1997, and Executive Order 13526 are examples of authorities that limit what can be shared with unauthorized individuals. These laws and order, for example, contain prohibitions on disclosure of items like certain privacy related information, source selection information, contractor proposal information, and classified information. Employees should not disclose nonpublic information through social media activities.

In addition, the [Standards of Ethical Conduct for Employees of the Executive Branch](#) states that you may not allow the improper use of nonpublic information to further your own private interest or that of another, whether through advice or recommendation or by knowing unauthorized disclosure. Nonpublic information is information that you receive because of your Federal employment that you know or reasonably should know has not been made available to the general public.

Some examples of nonpublic information are:

- information covered under the Privacy Act,
- classified information,
- proprietary information from private sector vendors or contractors,
- information designated as exempt under FOIA,
- source selection information on contracts or grants, and
- confidential Business Information as defined by Federal law.

Remember, what is true on the phone, snail mail or email is equally true using social media. If it is not public information, it should not appear on GSA's social media sites.

About Endorsements of Products, Services, or Enterprises

Employees are reminded that they cannot use or allow the use of their Government position, title, or any authority associated with their public office to endorse any product, service, or enterprise. This restriction applies to both GSA employees using social media in their official capacity as well as GSA employees' personal use of social media. The use of GSA social media accounts and tools in an official capacity is part of the authority associated with your public office. For example, a GSA employee who is using social media in his or her official capacity, could not post a statement saying "GSA should negotiate a terms of service agreement with Twitter, because Twitter is the best platform for public communication." This statement endorses Twitter by stating that Twitter is the best platform for communication. However, a GSA employee, who is using social media in his or her official capacity, could post a statement such as "GSA just negotiated a terms of service agreement with Twitter, which will provide GSA with a platform to communicate with the public." This second statement is a statement of fact versus an opinion and an endorsement. Employees must avoid endorsing or appearing to endorse any private interests or non-Federal groups.

Section 508 Standards (Accessibility)

Section 508 of the Rehabilitation Act of 1973, as amended, requires that electronic and information technologies purchased, maintained, or used by the Federal Government meet certain accessibility standards. These standards are designed to make online information and services fully available to the 54 million Americans who have disabilities, many of whom cannot possibly access information that does not comply with the Section 508 standards. Agencies are already required by the Federal Acquisition Regulation to modify acquisition planning procedures to ensure that the 508 Standards are properly considered, and to include the standards in requirements documents. OMB reminds agencies to disseminate information to the public on a timely and equitable basis, specifically mentioning meeting the Section 508 requirements in [OMB Memorandum M-06-02](#).

Agencies employing non-Federal social media services are required to ensure that persons with disabilities have equal access to those services. Please use this [handy checklist](#) to ensure the accessibility of your content. Contact your [GSA Section 508 Coordinator](#) if you have any questions or complaints.

Resources: [Section508.gov](#), [OMB Memo M-06-02](#), [Section508 Standards](#).

Practice Proper Records Management

When using electronic media, whether it is a blog, a website, a wiki, email, or any other type of electronic communication, the regulations that govern proper management, archival, and release of records still apply. The National Archives and Records Administration (NARA) offers resources and guidance to agencies to ensure proper records management. Contact records@gsa.gov for questions pertaining to records management at GSA.

Resources:

- [OMB Circular A-130, "Management of Federal Information Resources"](#).
- NARA regulations and guidance, including [Implications of Recent Web Technologies for NARA Web Guidance](#),
- NARA Bulletin 2010-05, September 08, 2010, "[Guidance on Managing Records in Cloud Computing Environments](#)" , and
- [NARA Guidance on Managing Records in Web 2.0/Social Media Platforms](#) .

Know the Laws for Information Collection

Agencies are required, when practicable, to use electronic forms and filing to conduct official business with the public, and social media technologies can be used in many cases to meet this need. Federal public websites are required to ensure that information collected from the public minimizes burden and maximizes public utility. The Paperwork Reduction Act (PRA) covers the collection of data from the public. The PRA requires OMB approval of all surveys given to ten (10) or more participants. This includes any sort of survey where identical questions are given to ten or more participants, regardless of the format. The exception to the survey rule is an anonymous submission form where users can provide open ended comments or suggestions without any sort of Government guidance on the content. The Children's Online Privacy Protection Act also has prohibitions and requirements regarding communication and collection of data from people under the age of 13. Questions about the applicability of these acts may be directed to the Office of the Chief Information Officer's IT Policy & Compliance Division and the Office of General Counsel.

Resources:

- [Government Paperwork Elimination Act](#),
- [Paperwork Reduction Act](#) , and
- [Children's Online Privacy Protection Act](#),
- [2010 OMB Memo on Social Media, Interactive Technologies and the Paperwork Reduction Act](#)

Plain Language

The Plain Writing Act of 2010 requires the federal government to write all new publications, forms, and publicly distributed documents in a "clear, concise, well-organized" manner. Visit www.plainlanguage.gov for examples of Plain Language and information on free training.

Meet Information Quality Standards

The public places a high degree of trust in ".gov" content and considers it an authoritative source. Under the [Information Quality Act](#), agencies are required to maximize the quality, objectivity, utility, and integrity of information and services provided to the public. With regard to social media information dissemination products, agencies are required to reasonably ensure suitable information and service quality consistent with the level of importance of the information. Reasonable steps include: 1) clearly identifying the benefits and limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity), and 2) taking reasonable steps to remove the limitations

inherent in the product or information produced. Agency management should ensure that the Agency position, rather than one person's opinion, is reflected in all communications. Resource: [Information Quality Act, Pub. L. No. 106-554](#).

Ensure Meaningful Access by People with Limited English Proficiency

Executive Order 13166 requires that persons with limited English proficiency (LEP) have meaningful access to an Agency's federally conducted programs and activities in order to prevent national origin discrimination. The use of social media technologies to communicate and collaborate with citizens is a federally conducted activity.

To ensure meaningful access by LEP individuals, an Agency must conduct a flexible and fact-dependent individualized assessment that balances four factors: (1) the number or proportion of eligible LEP persons; (2) the frequency of contact; (3) the nature and importance of the program or activity; and (4) the availability of resources. Based on this four-factor analysis, an organization must develop and implement an LEP plan if it determines a need for such a plan. This framework was established by the U.S. Department of Justice (DOJ) pursuant to Executive Order 13166 to federal agencies on the implementation of and compliance with this order. For more information on LEP at GSA, please contact GSA's Office of Civil Rights (OCR) at (202) 501-0767 or review the following information at [OCR's website library](#) on LEP. DOJ's guidance and other information/resources can be accessed at [lep.gov](#) and [LEP Frequently asked Questions](#).

Protect Intellectual Property

The use and management of social media technologies raises several questions about the legal concepts of copyright, fair use, and intellectual property ownership. Agencies should be diligent to ensure that they consider existing intellectual property and copyright laws when implementing social media technologies. While the Federal Government typically provides public data that is not considered copyrightable intellectual property, social media technologies that allow public contribution of content may potentially create challenges regarding the protection of intellectual property contributed by visitors. Agencies are required to post clear disclaimers detailing the copyrights that non-government contributors to their sites may retain. Government content can sometimes belong to the public domain and therefore be free from copyright, but this is not always true, especially when images and trademarked names or logos are concerned. Thus, this content cannot automatically be assumed to be free of intellectual property rights and available for any individual or site provider wishing to use it. Social media can make it easy to violate another's rights, so employees need to ensure they do not infringe on another's protected rights. Also, employees should post clear disclaimers detailing liability if a member of the public's post violates another's intellectual property or copyright. The GSA Star Mark is registered with the U.S. Patent and Trademark Office and the GSA Seal is protected by statute. [Guidance](#) on using GSA's branding images can be found on GSA's InSite. Specific questions should be directed to the Office of General Counsel.

Resources: [Copyright.gov](#), [U.S. Trademark Law](#).

Privacy Considerations

The Government requires public-facing websites to conduct privacy impact assessments if they collect personally identifiable information. They should post a "Privacy Act Statement" that describes the Agency's legal authority for collecting personal data and how the data will be used. Privacy policies on each website are also required in a standardized machine-readable format such as the Platform for Privacy Preferences Project, or P3P. Information on Web 2.0 platforms is accessible by others, so do not disclose Privacy Act protected information or other personally identifiable information unless authorized to do so in that medium.

Resource: [GSA's Privacy Program](#).

Cookies

Many social media tools use "persistent cookie" technology. A persistent cookie is a small text file that a website places on a visitor's computer so that it can remember the visitor when they show up again later. In general, websites use cookies for things like a "Remember Me" checkbox that lets you quickly log into a website, or to get metrics on site usage to understand how people are using the site. The most recent guidance from OMB on the use of persistent cookies by Federal agencies is [OMB Memorandum-10-22](#). It differentiates between "Tier 1" and "Tier 2" cookies, which do not collect users' personal information, and "Tier 3" cookies, which do, and thus require a more extensive review and public comment process. Another resource is [OMB Memorandum-10-23](#) which provides guidance for Agency Use of Third-Party Websites and Applications.

Provide Data in a Usable Format

Many social media technologies allow users to take data from one website and combine it with data from another, commonly referred to as "Mashups." Agency public websites are required, to the extent practicable and necessary, to achieve intended purposes, to provide all data in an open, industry standard format that permits users to aggregate, disaggregate, or otherwise manipulate and analyze the data to meet their needs. Agencies need to ensure that these open industry standard formats are followed to maximize the utility of their data.

Resource: [OMB Memorandum M-05-04](#).

Adhere to Lobbying Rules

18 USC 1913 prohibits the use of appropriated funds for purposes of lobbying a member of Congress. Such funds may not be "used directly or indirectly to pay for any personal service, advertisement, telegram, telephone, letter, printed or written matter, or other device, intended or designed to influence in any manner a Member of Congress, a jurisdiction, or an official of any government to favor, adopt, or oppose, by vote or otherwise, any legislation, law, ratification, policy, or appropriation, whether before or after the introduction of any bill, measure, or resolution proposing such legislation, law, ratification, policy, or appropriation...". The use of appropriated funds may extend to the payment of employees salaries, equipment, office space, and so forth. Federal employees should be mindful of 18 USC 1913 when using social media as the same restrictions apply. Please refer any questions to GSA's Office of General Counsel.

Resource: [OMB Policies for Federal Public Websites](#).

Avoid Political Activity (Hatch Act)

Even though social media is widely used in politics, the general rules that apply to Government communications haven't changed. Take caution to avoid any topics that may violate the Hatch Act. Employees are reminded that the Hatch Act prohibits them from engaging in certain political activity. Specifically, the Hatch Act prohibits employees from being politically active while on duty; while in any room or building occupied in the discharge of official duties by an individual employed or holding office in the Government of the United States, or any Agency or instrumentality thereof; while wearing a uniform or similar item that identifies their employing Agency; or while using a government vehicle. Political activity is defined as any activity directed towards the success or failure of a political party, candidate for partisan political office, or partisan political group. In addition, employees may not use their official title while participating in political activity, may not use their authority to coerce any person to participate in political activity, and may not solicit or receive political contributions. Likewise, the same rules apply to using social media to engage in political activity while you are on duty. For more information on the Hatch Act, please visit the [Office of Special Council's website](#), and look [here](#) for specific answers to frequently asked questions on this topic. Employees are also encouraged to seek guidance from the GSA's Office of General Counsel.

Know When the Federal Advisory Committee Act Applies

Since many social media technologies excel at enabling information sharing across the Internet, Government programs may use them to share ideas regarding current and future plans, to gather opinions about a wide variety of issues and to strengthen the relationship between citizens and their Government. Depending on circumstances (such as targeting specific experts for an online discussion of proposed policy), some of these efforts, depending on how they are structured, may meet the functional definition of a virtual or electronic advisory group and therefore fall under the purview of the Federal Advisory Committee Act (FACA). Just because a FACA meeting is held in virtual space instead of office space, it is not exempt from the Government's rules on such activities.

Any advisory group, with limited exceptions, that is established or utilized by a Federal Agency and that has at least one member who is not a Federal employee, is required to comply with the FACA. In general, when Government agencies seek input and suggestions from the general public on various issues, FACA likely will not apply. However, if the Government is managing and controlling the group in any way, such as selecting members, setting an agenda, or consolidating results generated by the group of participants, the group will fall within the bounds of FACA. To find out if a group comes under the FACA, any individual may contact the sponsoring Agency's Committee Management Officer, or the GSA Committee Management Secretariat.

Resource: [Federal Advisory Committee Act](#).

Monitor What You Control

Social media users are responsible for continually checking the pages that they own. The person who has responsibility for approving the page, or their designee, should ensure the

information is accurate, timely, relevant, complete, and does not adversely affect the execution of the mission and responsibilities of GSA or the Federal Government. This responsibility includes inactivating the page upon the owner's termination and/or notifying the Office of the Chief Information Officer (OCIO) that the page has been transferred to another individual. Questions may be directed to socialmedia@gsa.gov.

6: GSA Encourages and Supports Social Media

Social media tools have been increasingly used by GSA to communicate with citizens and our customers. They can continue to rise in importance as a communications channel if we follow some basic procedural principles. For example, a "Blog Request Form" (<http://insite.gsa.gov/blogrequest>) is used to initiate a blog, which will be processed by the OCIO's Enterprise Applications Division. Blog requests at GSA should:

- Clearly define the subject matter that will be the focus of your blog;
- Provide some basic metrics that will be used to measure whether your blog is effective (e.g., posts per week, comments per post, etc.); and
- Define how, if at all, your blog will relate to other social media channels already created by GSA or organizations within GSA.

See Appendix D Guidance for Bloggers.

Before You Start using social media tools such as Twitter, Facebook or YouTube, here are a few things to keep in mind:

- GSA's social media policy applies to any message written in your official capacity or with the express purpose of communicating about GSA's business and mission.
- **Apps.gov** provides a host of free third-party tools with which GSA has signed an amended "fed-friendly" Terms of Service agreement. These tools are **not** necessarily compliant with Federal accessibility, privacy, and security laws out-of-the-box, so it is your responsibility to ensure that they are used in a compliant way.
- **The Citizen Engagement Platform (citizen.apps.gov)**, hosted by GSA, provides Federal employees at all agencies with a fast and easy way to create a blog. The tools hosted by the CEP, including a WordPress blogging platform, *are* compliant out-of-the-box with all current Federal policies on privacy, security, accessibility, and others.

7: Social Media Use Should Be Strategic

Whether you use Apps.gov or commercial sites such as Facebook and Twitter, social media presents opportunities for supplementing how GSA reaches its target audiences, such as citizens. Social media tools should never replace official communication channels, such as gsa.gov, for disseminating information. Because these sites evolve at a rapid pace, how to best incorporate them will need to be tailored to your organization's needs, its business strategy and its overall communications strategy. Remember, agencies are required to ensure Government information is available and accessible to people without Internet connectivity, so you must provide members of the public who do not have Internet

connectivity with timely and equitable access to information, for example, by providing hard copies of reports and forms.

8: GSA Has the Right to Monitor and Remove Comments

GSA recognizes the public's First Amendment rights and will allow various comments, viewpoints, and opinions. In fact, social media usage is designed to solicit that input. However, GSA is allowed to monitor and remove some public comments that are political, target specific individuals or groups, are abusive, or are similarly unacceptable. In many situations, a posting policy and/or rules of use policy is needed for the GSA social media presence. Individuals should contact the Office of General Counsel as situations arise that may require the monitoring or removal of comments posted on or to a GSA social media presence.

9: This Guide Will Continue to Be Reviewed

This Guide will be reviewed at least every year by the Offices of the Chief Information Officer, General Counsel, Governmentwide Policy, and Citizen Services and Innovative Technologies. The purpose of this review will be to incorporate changes in available technologies and relevant practices and policies.

APPENDIX:

A. Requirements Checklist When Using Social Media

This is a quick reference to the applicable requirements to fulfill when you are using social media tools in your official capacity as a GSA employee.

Compliant?	Federal Information Requirement
	<p>GSA Sponsored Blog Guidelines Guidelines for creating and maintaining a GSA sponsored blog may also be applicable to other GSA sponsored social media (e.g., wikis). The OCIO supports enterprise operations and the Office of Citizen Services and Innovative Technologies (OCS IT) oversees editorial use. Resource: socialmedia@gsa.gov.</p>
	<p>Commercial Sites Commercial sites are opportunities for supplementing how GSA reaches its target audiences, such as citizens. They should not replace official communication channels, such as gsa.gov.</p>
	<p>Section 508 If the dissemination of information in an accessible manner constitutes an undue burden on the Agency, the Agency is required to make the information available in alternative formats for individuals with disabilities. Resources: GSA Section 508 Coordinator, Section 508 of the Rehabilitation Act, OMB Memo M-06-02.</p>
	<p>Records management, retention and archiving The regulations that govern proper management, archiving, and release of records still apply. Determine the most appropriate methods to capture and retain records on both Government servers and technologies hosted on non-Federal hosts. Resources: records@gsa.gov, OMB Circular A-130, "Management of Federal Information Resources," section 8a4, Implications of Recent Web Technologies for NARA Web Guidance and NARA Guidance on Managing Records in Web 2.0/Social Media Platforms.</p>
	<p>Plain Language The Plain Writing Act requires the federal government to write all new publications, forms, and publicly distributed documents in a "clear, concise, well-organized" manner. Resource: www.plainlanguage.gov.</p>
	<p>Information Quality Agencies are required to reasonably ensure suitable information and service quality consistent with the level of importance of the information. Agency management is required to ensure that the Agency position (rather than one person's opinion) is reflected in all communications. Resource: Information Quality Act, Pub. L. No. 106-554.</p>
	<p>Availability to Persons with Limited English Proficiency Executive Order 13166 requires that agencies take reasonable steps to ensure meaningful access to their Federally conducted programs and activities by persons with limited English proficiency (LEP). Resource: Office of Civil Right's library.</p>
	<p>Usability of Data Agency public websites are required, to the extent practicable and necessary to achieve intended purposes, to provide all data in an open, industry standard format that permits users to aggregate, disaggregate, or otherwise manipulate and analyze the data to meet their needs. Resource: OMB Memo M-05-04</p>
	<p>Intellectual Property Agencies are required to post clear disclaimers detailing the copyrights that non-Government contributors to their sites may retain. Resources: Copyright.gov, U.S. Trademark.</p>
	<p>Privacy The Privacy Act of 1974 (as amended) may also apply to the activities undertaken on social media platforms, and individuals should consult with the GSA Privacy Office and OGC to ensure they are in compliance with all privacy protection requirements. Resource: GSA's Privacy Program.</p>
	<p>Federal Advisory Committee Act Some of these efforts, depending on how they are structured, may meet the functional definition of a virtual or electronic advisory group and therefore fall under the purview of FACA. Resource: FACA.</p>
	<p>Information Collection & Paperwork Reduction Act The Paperwork Reduction Act (PRA) covers the collection of data from the public. The PRA requires OMB approval of all surveys given to ten (10) or more participants. This includes any sort of survey where</p>

identical questions are given to ten or more participants, regardless of the format. Resources: Government Paperwork Elimination Act and Paperwork Reduction Act .

B. More Advice for Engaging in Online Conversations

It's a Smart Idea to Engage Regularly and Respond Quickly

In social media, conversations take place over minutes or hours, not weeks or months. If you decide to engage in conversation using social media, be sure that you are able to respond quickly and with all the facts. Even if your reaction is "we can't provide an answer yet," providing some response quickly is part of the excellent customer service all citizens should receive when talking to a GSA employee. If you host a blog, be sure you dedicate the resources needed to provide new content on a regular basis.

Don't Be Afraid to Ask For Input When You Need It

It's great to involve citizens in the governing process by asking for ideas or input. Before you do, make sure you're asking about an issue where you can actually be responsive to outside suggestions. For example, you may want to ask whether your visitors would find a new website feature helpful, but you would avoid asking whether another Agency's website should be redesigned. Citizens expect us to operate Government effectively, and part of doing that is asking for feedback when appropriate.

Try to Be as Transparent as Possible

It's great to share as much useful information as you reasonably can, so that citizens understand what their Government is doing and why. However, every day, GSA employees are trusted with information that isn't appropriate for sharing with the public, such as the status of an ongoing procurement or negotiations over a building lease. If you're unsure whether something can be shared, talk to your supervisor or security manager.

Remember to Engage for Accuracy, not Argument

Because of the many important issues GSA handles, there's a lot of conversation about us online. (For example, head to Twitter.com and search for "General Services Administration" to see what people are saying about us right now!) If you see misrepresentations made about GSA in social media, you can certainly use your social media site or someone else's to point out the error and provide correct facts. Make sure your position is factual, and not disparaging or argumentative in tone.

Don't Hesitate to Admit Mistakes Quickly

Part of honestly engaging with citizens is admitting when you've made an error. If you make an error, be upfront about the mistake and correct it quickly. If you choose to modify something you said earlier, make clear what you are modifying, and make it clear that you have done so (e.g. by using ~~strikeru~~ strikethrough text). Nobody expects you to never make a mistake; we do expect you to be honest and upfront about it when you do.

A Good Rule of Thumb About Social Media Communication

Say to citizens on social media only that which you would say on the phone or in other official communications. There are always consequences to what you write. If you're unsure about something, discuss your proposed post with your supervisor.

C. Frequently Asked Questions

Q: Can I use social media tools (both GSA-sponsored and third party sites such as <http://facebook.com> or <http://twitter.com>) in my official capacity as it relates to my job and job function?

A: Yes, you may use both GSA-sponsored and third party sites to help get the Agency's message out to people. Keep in mind that the rules which govern official GSA communications, such as the Standards of Ethical Conduct for Employees of the Executive Branch, still apply. Also, use caution to avoid accepting the standard "click-through" User Agreement on most websites as they contain provisions that the Government cannot legally accept. Appendix E provides guidance related to risks and mitigation strategies.

Q: Does GSA's Social Media Policy require that GSA offices must use social media tools?

A: There is no requirement that GSA offices must use social media tools like Facebook. The GSA Social Media Policy encourages the use of social media technologies to enhance communication, collaboration, and information exchange in support of GSA's mission.

Q: As part of my official responsibilities, I am responsible for administering my office's blog. What can't I talk about on the blog?

A: Your office's efforts with social media should always be related to GSA's mission, so you should always keep your message strategic and focused. Follow the same rules using your office's blog that you use with any other means by which this Agency communicates with the public (telephone, internet web sites, etc.). These rules cover endorsements, appropriate language, political statements, and other topics. See Appendix D Guidance for Bloggers.

Q: As part of my official duties, I am responsible for maintaining one of my office's Facebook pages. Are there any Facebook-specific rules I need to be aware of?

A: There are no new rules to follow as a result of using Facebook or other social media tools. The guidelines for appropriate use of social media already exist in rules that apply to official communication.

Q: A web service like Twitter isn't compliant with Section 508, yet GSA offices use it to communicate. Why is that allowed?

A: Commercial sites like Twitter are opportunities for supplementing how GSA reaches its target audiences. They should not, however, completely replace official communication channels, such as gsa.gov. GSA offices using Twitter make the information in their posts available through official channels that meet all legal requirements. Increasingly sites like www.accessibletwitter.com are being used to ensure that content is accessible to all. Generally speaking, as long as there is equal access to the information for people with and without disabilities, and commercial sites are not the only or official source of GSA information, GSA offices may communicate using sites like Twitter or Facebook.

Q: Is GSA's Social Media Navigator a step toward limiting what GSA employees can say on GSA's Facebook, YouTube, and Twitter pages in their official capacity?

A: No. This Guide provides guidance on how to use social media tools, such as Facebook, YouTube and Twitter, in carrying out GSA's mission while still complying with applicable rules and regulations. Social media is just another communications tool. When speaking in your official capacity, the same rules apply whether you communicate through social media or another means of communication such as the telephone or gsa.gov.

Q: I want to set up an official blog, Facebook page or Twitter account for my office. Do I need permission, and whom should I ask?

A: You should speak to the person in your office that has executive oversight or responsibility for the subject about which you will be communicating. Also, please notify the Office of Communications and Marketing at socialmedia@gsa.gov, so that they can maintain an updated list of GSA's social media presences.

Q: I must admit I don't know much about Facebook or Twitter and wondered if you have any really specific guidance on using them?

A: As a matter of fact, the people in the Office of Enterprise Web Management in the Office of Communications and Marketing have been answering questions just like yours when they receive e-mails at socialmedia@gsa.gov. They have created two very helpful handouts—one for using Twitter and the other for Facebook. Check them out here:

[Guidance for Twitter Accounts](#)

[Guidance for Facebook Accounts](#)

D. Guidance for Bloggers

Blogs succeed when visitors feel they have reached a trusted source of information. Let readers know who the blogger is from a professional standpoint. Do not release any personal information that the general public should not know, for example a home address or phone number.

Be prepared to post content on a regular basis. This may mean daily or weekly, but not less frequently than every two weeks. Let readers know what the posting schedule is. Be realistic in preparing a schedule. It is always better to increase frequency over the life of a blog. If a blog remains idle for 60 days or more, GSA reserves the right to take it offline.

Be prepared to make time and devote resources to moderating all comments that readers post. Be committed to read every comment received, even if nothing is posted in response to it. Time may be needed to research responses. Communicate to the audience the timeframe within which the comment may be posted.

Invite guest contributors. This is a great way to enhance value without increasing workload. Announce in advance who the guest contributors will be.

Be prepared to respond on the blog to the posted comments, especially negative ones. Blogs build credibility and readership when they are as open as possible.

If the same questions are posed over and over again, consider creating boilerplate responses to the questions.

A blog should adhere to [GSA Order, GSA Logo And Visual System \(CSC 1808.1\)](#), which states, "the GSA Star Mark... will be used on all stationery, business cards, print and electronic communications products throughout the agency."

Be aware that there are a variety of ways people will find the blog (e.g., via search engines, search and other e-mail alerts, RSS feeds, various social networking sites, book marking sites, and e-mail from another person). This means that individuals will often read only a headline (or title), or a headline and a couple of sentences. The more intriguing and relevant the headline of the blog and the content that follows, the more likely the content is to build readership.

Blog Posting Requirements and Disclaimers

All GSA blogs should contain the entire notice listed below. If the notice itself is not on the main page, then a prominent link should be on the blog homepage that clearly identifies the attachment as "Privacy, Security, and Legal Notice." The sections below identify required statements and disclaimers for GSA sponsored blogs. These statements, or links to pages containing them, should be located on the main page of every GSA sponsored blog.

(1) General policy. The U.S. General Services Administration (GSA) manages this blog to provide a forum for improving communications with our employees, Government customers, our commercial suppliers, and the general public. This blog will discuss (subject matter of blog, e.g. information technology, schedules, communications, building issues, etc.). This blog use policy is subject to amendment or modification at any time to ensure the blog's continued use is consistent with its intended purpose as a limited forum.

(2) Posting policy. You are encouraged to share your comments, ideas, and concerns. This is a moderated blog, and GSA will only post comments from bloggers over 13 years of age that relate to topics on (Blog Subject Matter). GSA will review all comments before posting them. GSA will not post comments that contain abusive, vulgar, offensive, threatening or harassing language, personal attacks of any kind, or offensive terms that target specific individuals or groups. GSA will not post comments that are clearly off-topic, that promote services or products, or that promote or oppose any political party, person campaigning for elected office, or any ballot proposition. Gratuitous links to sites are viewed as spam and may result in the comment being removed. Communications made through the blog's e-mail and messaging system will in no way constitute a legal or official notice or comment to GSA or to any official or employee of GSA for any purpose. The content of all comments are released into the public domain unless the commenter clearly states otherwise, so do not submit anything you do not wish to be broadcast to the general public. GSA does not discriminate against any views, but reserves the right not to post comments that do not adhere to these standards. GSA will make best efforts to review comments and post them as quickly as possible.

(3) Product references by blog host. Any references to commercial entities, products, services, or other non-Governmental organizations or individuals that are included in this blog are provided solely for the information of individuals using this blog. These references are not intended to reflect the opinion of GSA, the United States Government (Government), or its officers or employees concerning the significance, priority, or importance to be given the referenced entity, product, service, or organization. Such references are not an official or personal endorsement of any product, person, or service, and may not be quoted or reproduced for the purpose of stating or implying GSA or Government endorsement or approval of any product, person, or service.

(4) Records management. All blogs conform and comply with the Agency's records maintenance and disposition system.

(5) Linking policy. The (Blog Name) blog may include useful hypertext links or pointers to information created and maintained by other public and private organizations and individuals' blogs. All hypertext links conform to all points in Section 6. (Blog Name) provides these links and pointers solely for the blog users' information and convenience.

When a user selects a link to an outside website, he/she is leaving the (Blog Name) blog and is subject to the privacy and security policies of the owner/sponsor of the outside website. Hyperlinks to information created and maintained by other public and private organizations should not be construed as an endorsement of the views or privacy policies contained on those linked pages.

(a) GSA and (Blog Name) **do not** control or guarantee the accuracy, relevance, timeliness or completeness of information contained on a linked website.

(b) GSA and (Blog Name) **do not** endorse the organizations sponsoring linked websites, and do not endorse the views they express or the products/services they offer.

(c) GSA and (Blog Name) **cannot** authorize the use of copyrighted materials contained in linked websites. Request such authorization from the sponsor of the linked website. Those who provide comments are responsible for the copyright of the text they provide.

(d) GSA and (Blog Name) **are not** responsible for transmissions users receive from linked websites.

(e) GSA and (Blog Name) **do not** guarantee that outside websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

(6) Copyright information. Links to GSA blogs are welcomed. Unless a copyright is indicated, information on GSA's blogs is in the public domain and may be copied and distributed without permission. Citation to the U.S. General Services Administration as the source of the information is appreciated.

If a copyright is indicated on a video, photo, graphic, or other material, obtain permission to copy the material from the original source.

(7) Public affairs. If you would like verification or a transcript of information released on GSA blogs or if you have any questions or comments about the information presented, please contact GSA's Office of Communications and Marketing's Public Affairs Office. Reporters can submit questions to the Public Affairs Office through normal query channels; they should refrain from submitting questions on blogs as comments. GSA will not post questions from reporters. Public Affairs may be contacted at 202-501-1231.

(8) Privacy. (Blog Name) follows the gsa.gov privacy policy. GSA will not share or sell any personal information obtained from users with any other organization or Government Agency except as required by law. Please view our complete Privacy and Security Policy. To protect your own privacy, and the privacy of others, please do not include phone numbers, e-mail addresses, or other personal information in the body of your comment.

(Blog Name) is unable to post comments from children under the age of 13 due to the Children's Online Privacy Protection Act (COPPA). If you are 12 years old or

younger, you may email us rather than posting a comment on (Blog Name).

The (Blog Host Office Name) manages this blog as a portal for information from the U.S. General Services Administration. However, information posted on this blog is not official policy of GSA and will in no way grant anyone any rights, privileges, or standing on any matter. All information should be verified through official channels at GSA. For employee contact information at GSA, please check <http://www.gsa.gov/contacts>.

E. Risks And Mitigation Strategies

The safe use of social media is fundamentally a behavioral issue, not a technology issue. Accordingly, the decision to embrace social media technology is a risk-based decision, not a technology-based decision. Social media sites are not, for the most part, any more or less inherently insecure than other types of web applications. Many of these technologies are operated by third parties (e.g., Facebook, YouTube, and Twitter); they therefore may be prone to security vulnerabilities. Since the social media technologies are used by GSA programs for public-facing interaction of outreach and marketing, FISMA or similar security risk assessments and standards that are normally applied to Government-operated IT systems are not considered applicable. Guidance for performing due diligence when considering official use of social media beyond outreach and marketing purposes is available through the Senior Agency Security Officer in the Office of the Chief Information Officer.

To ensure that GSA's use of social media is both safe and effective, this document provides GSA-specific guidelines and recommendations for mitigating security risks posed by social media tools and protecting the GSA network. Because this landscape is constantly shifting, these recommendations and risks are only as good as the latest draft and should not be considered exhaustive or comprehensive. As we learn more from our experiences and yours, we will regularly update this document to reflect the best practices to secure our network and still uphold GSA's mission.

1. Types of Risks:

Social media technologies such as wikis, blogs, and social networks are vulnerable to three types of cyber attacks: Spear Phishing, Social Engineering, and Web Application Attacks.

Spear Phishing is an attack targeting a specific user or group of users that attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Participants in social media should be careful in clicking on links and communicating with other members of online groups.

- **Social Engineering** relies on exploiting the human element of trust. 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.
- **Web Application Attacks** are dynamic web pages that use scripting to provide additional functionality to the user. Social media websites are advanced web applications, and this opens them up to a wide range of vulnerabilities exploitable by attackers. 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 Facebook applications to target users. Facebook applications are written by third-party developers and often have minimal security controls.

2. Strategies for Minimizing Risk

The risks outlined above are serious, but they should not be a reason or an excuse not to use social media. While launching an attack like these is technically complex, all you need to avoid them is a little bit of knowledge and common sense. Below are some strategies that you can use to minimize risk and use social media safely and a sample risk mitigation checklist. *(These guidelines are adapted from the Federal CIO Council's document, "[Guidelines for Secure Social Media Policy](#)," This list is abbreviated; you should consult the original document for more complete guidance.)*

Procedural Controls

The most important question in ensuring the safe use of social media tools is not "what tools do we use?" but "how do we use them?" Any use of social media should be accompanied by some thoughtful operating procedures. Be explicit about the type of data or information you will share. Who is authorized to post content? Who is authorized to approve it? Prepare a brief document that captures your goals and objectives for use of social media, and accordingly, what types of interactions you are and are not seeking to engage in. Create operating procedures 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.

Acquisition Controls

Most social media services provide administrative features that can customize how information is collected from and provided to the public, either bundled with the service or for an additional fee. A great example of this is GSA's own Terms of Service (TOS) agreements with social media providers (see the "Social Media Apps" section of www.apps.gov), many of which include negotiated terms for IT security. Consider comparing the feature sets of platforms side-by-side, or engaging vendors to inquire about the security and privacy features they provide. Consider whether platforms that use voting or public comment are prone to being "gamed" or invite cheating or fraud, and what measures can be taken to prevent it.

Training Controls

The key to using social media securely is ensuring that everyone who uses it has access to sufficient training materials and opportunities. Even for social media initiatives that are not new, providing periodic awareness and training can help educate users about what information to share, with whom they can share it, and what not to share. Employees should also be trained to protect both GSA and themselves by avoiding blurring their personal and professional lives, and with additional guidance concerning if and how they should identify themselves on social media websites, depending on their official role. GSA's Office of the Chief Information Officer (OCIO) also operates a number of **network controls** and **host controls** aimed at safeguarding GSA's information and networks.

Sample Social Media Risk Mitigation Checklist

- Is a content disclaimer and site ownership disclaimer in place?
- Is there a plan for regular content updating and content review in place?
- Is a blog comment moderation policy in place?
- Has the staff responsible for creating and maintaining GSA content been briefed on the Social Media Policy and accompanying Guide?
- Is a plan for security vulnerability checks in place and is staff assigned the review?
- Has a written incident response plan been vetted and approved?
- Is a plan in place for regular review of things like:
 - Profile pages, to ensure that content is still correct and hasn't been compromised?
 - Friends' photos and other non-GSA controlled content on profile page, to ensure that it remains within reasonable guidelines?
 - Links, to ensure that destination pages have not been compromised and are not being used to promote attacks?
 - On-line vulnerability reports for the sites you are using?

F. How Agencies are Using Social Media

Social media lets anyone you talk to talk back to you just as easily. For Government, this presents some challenges, but also enormous opportunities. There is always room to improve how we deliver information and partner with stakeholders, and social media enables them to tell us—quickly and vocally—what we’re doing wrong and how we could be doing better. The feedback you get from social media can provide incredible insight into what our customers want and how we can deliver it. One great example is GSA’s own BetterBuy Project (https://betterbuy.fas.gsa.gov/index.php/Main_Page), a site that solicits ideas from across the country on how to make Federal acquisition more transparent and efficient. Thanks to that site, we’ve heard many new ideas, and implemented a few that have changed our acquisition customers’ experience for the better. There’s also [Challenge.gov](#), a site launched by GSA that lets agencies pose challenges to the public and reward innovative results. Even if you’re not engaged in active dialogue, you can still use social media to discover what others are saying about you and the services you provide. (Don’t believe it? Head to [Twitter.com](#) and search for “General Services Administration” to see what people are saying about us right now!) Many social media sites offer search functions that you can use to stay “ahead of the curve” and anticipate citizens’ ideas and needs.

Here are just a few of the literally hundreds of examples of agencies using social media to perform their mission and achieve great results:

- **Library of Congress on Flickr**—The Library is using social media not only to deliver its content in ways that all citizens expect and appreciate, but to enlist citizens in the critical mission of examining and cataloguing that content for future generations. In January 2008, the Library used the popular photo-sharing service Flickr (www.flickr.com) to put 3,000 public-domain, copyright-free photos online so that all citizens could share and explore them. Moreover, the Library used Flickr’s social tagging features to enable citizens to sort the photos by person, place, topic, and other key dimensions.
- **National Library of Medicine’s Pillbox**—Pillbox is a web application created by the National Library of Medicine that enables rapid identification of unknown pills by allowing a visitor to describe its shape, color, and markings and searching against Government data for a match. Useful for emergency physicians, first responders, health care providers, and concerned citizens, Pillbox is a great example of how the Internet can transform previously hard-to-access Government data into vital information that is at citizens’ fingertips.
- **TSA “Evolution of Security” Blog**—Blogging has represented a major shift in how we share and discuss information in real time. In January 2008, the Transportation Security Administration (TSA) recognized the potential value of this shift by launching the Evolution of Security Blog to provide “a forum for a lively, open discussion of TSA issues.” Since then, the blog has had thousands of posts and comments, and has become a model of how Federal Government can use blogs to engage authentically with citizens. The blog has also been used to provide travel

tips and clarify controversial incidents involving airport security, all the while building TSA's reputation for engaging in an honest and straightforward way with citizens.

- **Government Data Transformed into Apps**—Recent examples underline the creativity and innovation that is unleashed when Government data is made publicly available in open formats. In March 2010, USDA, in partnership with First Lady Michelle Obama's "Let's Move!" campaign to combat childhood obesity, launched the Apps for Healthy Kids contest to challenge developers and designers to build Internet or mobile applications, based on USDA nutrition datasets, that could teach children and young adults about how diet and exercise can affect their lives. The Institute of Medicine and HHS convened health care experts, technology developers, social media visionaries, to explore what could be done with HHS's community health data. The group brainstormed an incredible set of ideas – and then proceeded to develop more than a dozen new or improved data applications using HHS's community health."
- **TSA IdeaFactory**—Known as one of the most impactful internal collaboration tools in Government, TSA's IdeaFactory was launched in April 2007 with the goal of harnessing ideas from the over 40,000 front-line Transportation Security offers stationed at airports across the nation. In its first 18 months, the "IdeaFactory has grown from concept to a successful, widely-recognized innovation and collaboration program with approximately 40% participation across TSA ,over 9,000 ideas, resulting in the implementation of over 40 national programs and initiatives that have improved job satisfaction, increased retention and improved the quality of work life."
- **VHA/OIT Innovation Competition**—In addition to broad ideation, agencies are also finding ways to leverage targeted competitions and challenges to foster internal innovation. In February 2010, the Veterans Health Administration/Office of Information Technology launched the Innovation Competition, which challenged employees to suggest IT innovations that could enhance delivery of health services to the nation's veterans. The contest was wildly successful, garnering about 6,500 submissions from a participant pool of 45,000 participants—nearly a quarter of all eligible employees, according to VA Chief Technology Officer Peter Levin. In May 2010, VA announced 26 "winning ideas" that were selected for implementation, including: Reducing healthcare associated infections using informatics; a robust VA forms search engine; an E-discharge pilot program; and a touch screen device to support the nursing triage of patients.

The next innovation on this list could easily be yours! If you have a great idea and are not sure about where to take it, contact socialmedia@gsa.gov to get the assistance you need.