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

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 is 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.

    - 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.
    - 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 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
• 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.	• 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. phishing). • Using a compromised site to spread malware. • Acquiring confidential information about state employees or citizens (i.e. social engineering).

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):
  - TwInbox
  - 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

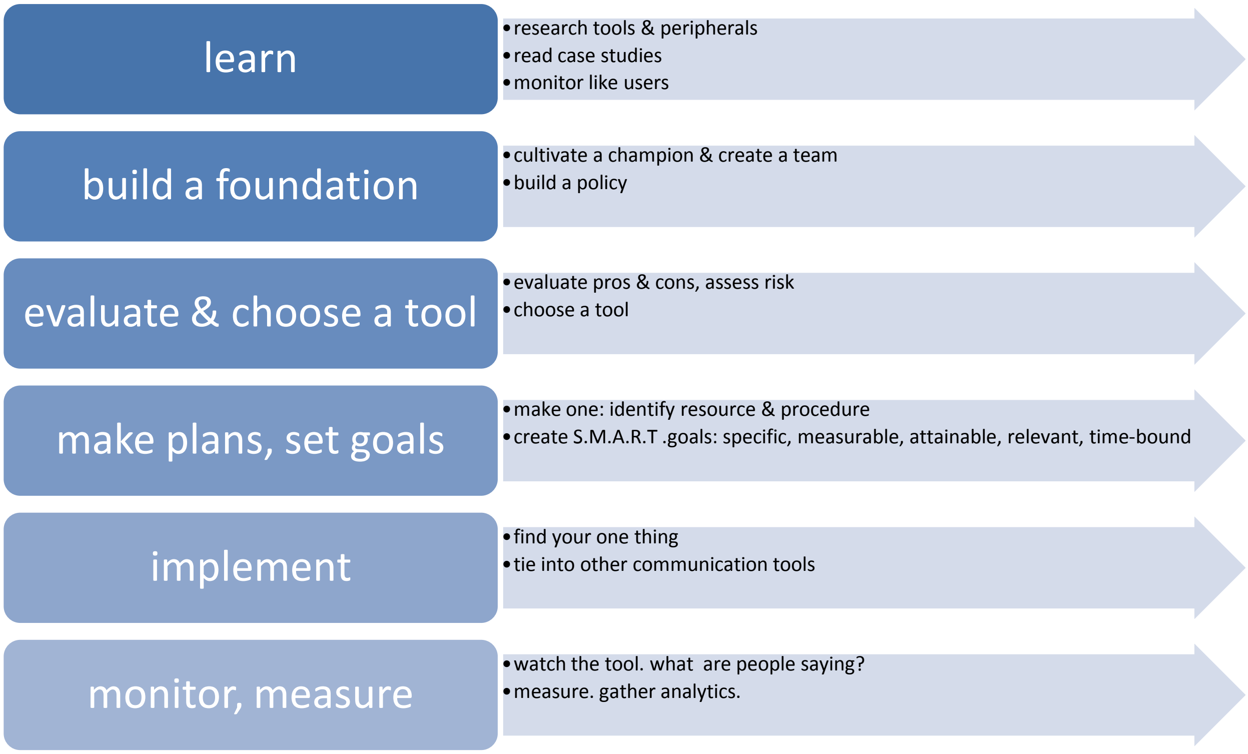
- CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies
- General Services Administration Social Media Handbook
- General Services Administration Social Media Policy
- IBM Social Computing Guidelines

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



learn

- research tools & peripherals
- read case studies
- monitor like users

build a foundation

- cultivate a champion & create a team
- build a policy

evaluate & choose a tool

- evaluate pros & cons, assess risk
- choose a tool

make plans, set goals

- make one: identify resource & procedure
- create S.M.A.R.T .goals: specific, measurable, attainable, relevant, time-bound

implement

- find your one thing
- tie into other communication tools

monitor, measure

- watch the tool. what are people saying?
- measure. gather analytics.

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