# Idaho Technology Authority (ITA)

# ENTERPRISE GUIDELINES – G300 INFORMATION AND DATA

## Category: G330 – BEST PRACTICES FOR UTILIZING SOCIAL NETWORKING SITES

**CONTENTS:**



## I. DEFINITIONS

Web 2.0: The term "**Web 2.0**" is commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. A Web 2.0 site gives its users the choice to interact or collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to websites where users are limited to the passive viewing of content that was created for them.

Social Networks: Websites that have been created to encourage users to join one or more networks and to allow the member-users to share ideas, activities, events, and interests within their individual networks.

As described by experts in Web 2.0 and Social Networks, the key elements of Web 2.0 are the following, using the acronym SLATES:

Search – finding information through powerful, broad-sweeping but relevant keyword explorations.
Links – connecting information together in a meaningful, interconnected network among collaborative entities.
Authorship – the ability for any user to create, update, and share content as part of an unbounded, collaborative network
Tags – categorizing content by attaching short descriptions (usually one word) to help organize information for activities such as searching.
Extensions – “mining” the collected user data which enables the web designer to lead users to similar or related activities or transactions (e.g., other customers who purchased this item also purchased…)
Signaling – the alerting of users or followers to content changes or updates in someone’s “status”

## II. RATIONALE

### A. Benefits of Social Networking Sites (SNSs):

Social software and SNSs provide a mechanism that enables individuals to dynamically interact with information in disparate formats. Additionally, these tools facilitate collaboration among users, often without regard to platform and geographical location. These tools allow users to store and access information vertically and horizontally within organizations. These tools provide a channel for the collection, the dissemination, and the utilization of information, which transcends traditional vertical business processes. The primary commodity in which modern government deals is information. These tools enable the agile handling of information.

Guidance in the utilization of SNSs and social software will result in a more consistent application and use of these tools.

### B. Security Concerns of SNSs:

**Malicious Software**

Social networking sites, particularly the more popular MySpace and Facebook have been used by criminal hackers to spread malicious software. Because the number of people on these sites has grown so quickly, a successful malware infection could yield great results for the criminals. Many malware infections, such as the dangerous Koobface malware, involved criminals posting a scam link to what is supposed to be a great video or news story. The link would connect to a malware site that would infect their computer or invite them to update their "flash player". These initial links were sometimes sent to other users through Groups rather than through Friends in order to ensure larger exposure. Once the user clicked on the link to update the flash player, their computer was infected with malware which would then ensure the scam link was reposted under their profile. The infected computer would then call home and download more nefarious malware which would turn the computer into a bot, steal information and yield the criminals their money. Other malware is spread through some of the many games that Facebook allows almost anyone to generate and share on the site. Facebook has a group intended to find and kill each and every virus dispersed on the site, but the initial spread can be so rapid that the only solution is to be sure users are aware that any Facebook message or application can be dangerous. If employees are using SNS, officially or personally, at work, these malware schemes introduce greater risk of malware on the state network and data breaches of state information.

**Social Engineering**

Another threat is through social engineering which becomes easier on a social site where information is shared freely with friends or groups. In 2009, 57% of social networking users reported they were spammed through one of the sites. One of the most disturbing social engineering risks is when a criminal poses as another person and invites people to be their friend. This has been common on professional networking sites as well as more popular social networking sites. Once the criminal has made a few friends, the circle starts growing and people share their private information with them. Sometimes the information available on a SNS is enough to steal and sell someone's identity, but often it's used to deliver more targeted invitations with links to malware sites or to sites which obtain work or banking account credentials. Sometimes the criminal will learn enough to guess or directly obtain SNS passwords and they will directly take over the accounts and send out attacks under their victim's profile.

**Official Data at Risk**

Employees using SNS are more likely to reveal information that is sensitive in nature than they are when using more traditional public relations media. This risk can be encouraged through "friends" who are actively socially engineering the employees and who ask specific questions after seemingly freely revealing their own sensitive information. All official SNS communications should be reviewed carefully to ensure sensitive information is not inadvertently released on open postings or "private" messages to contacts.

## III. GUIDELINE

**For agency employees that use social networking technologies as part of their job:**

It should be treated as a communication from the agencies to citizens, the same as other more traditional forms of communications (letters, press releases, interviews and email).

Below are guidelines for using social media. These guidelines are for employees or contractors creating or contributing to blogs, wikis, social networks, virtual worlds, or any other kind of social media both on and off state agencies websites. It is expected all who participate in social media on behalf of the state to be familiar with, understand and follow these guidelines.

### When You Engage

**ITA Professional Use:**

All agency-related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the agency's communications policy, practices, and expectations. Employees must not use social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Employees should be mindful that inappropriate usage of social media can be grounds for disciplinary action. If an account is used for business, the entire account, regardless of any personal views, is subject to these best practices guidelines, including the collection and preservation provisions.

**Be Clear As To Identity:**

Any employee using his or her name as part of a state agency's application of social media should be mindful of the following:

- Do not assume privacy. Only post information that you are comfortable disclosing;
- Use different passwords for different accounts (both social media and existing work accounts). Using the same password for multiple accounts increases the vulnerability of the accounts being compromised.

Emerging platforms for online collaboration are fundamentally changing the way we work, offering new ways to engage with customers, colleagues, and the world at large. It's a new model for interaction and we believe social computing can help you to build stronger, more successful relationships with citizens.

**If you are participating in social media:**

- Stick to your area of expertise;
- Post meaningful, respectful comments - no spam and no off-topic remarks or offensive remarks;
- Reply to comments in a timely manner, when a response is appropriate;

- Respect proprietary information and content, and confidentiality;
- When disagreeing with others' opinions, keep it appropriate and polite.

Follow all State and Agency Policies.

**Separate Personal and Professional Accounts:**
Employees should be mindful of not blurring the distinction between their personal and professional lives when administering social media sites.

**Personal Use:**
Employees are allowed to access personal social networking sites when not working. **Employees should never use their state e-mail account or password in conjunction with a personal social networking site nor should they display, use or copy any State logo. Further, Employees must ensure their personal social networking sites are separate and distinct from any official State site**. During normal business hours, employees may use personal social networking for limited family or personal communications so long as those communications do not interfere with their work or negatively impact the agency or state. Games are not authorized, as stated in ITA Policy, P1060, paragraph IV. 6., when using your work computer even when on personal time.

**Rules of Engagement**

**Be transparent**. Your honesty—or dishonesty—will be quickly noticed in the social media environment. If you are blogging, use your real name, identify where you work, and be clear about your role. If you have a vested interest in something you are discussing, be the first to point it out. You still need to keep confidentiality around information and content that is confidential.

**Be judicious**. Make sure your efforts to be transparent don't violate agencies' privacy, confidentiality, and legal guidelines. All statements must be true and not misleading and all claims must be substantiated and approved for publication. Never comment on anything related to legal matters, litigation, or any parties involved in litigation with or without the appropriate approval. What is published using social networking and Web 2.0 technologies is widely accessible and will be around for a long time, so consider the content carefully.

**Write what you know**. Make sure you write and post about your areas of responsibility and expertise. Respect brand, trademark, copyright, fair use, and confidentiality. If you have any questions about these get the appropriate permissions.

**Perception is reality**. In online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as a state employee, you are creating perceptions about your expertise and about the agency. Be sure that all content associated with you is consistent with your work and with the State's values and professional standards.

**Tone.** It is difficult to convey tone in online text, such as jokes and sarcasm, so their use should be used sparingly and in a manner that the reader will clearly understand.

**Context.** Make sure that statements are clear and minimize the possibility of text being taken out of context.

**It's a conversation**. Talk to your readers like you would talk to real people in professional situations. Consider content that's open-ended and invites response. Encourage comments. You can also

broaden the conversation by citing others who are blogging about the same topic and allowing your content to be shared or syndicated.

**Are you adding value**? There are millions of words out there. The best way to get yours read is to write things that people will value. Social communication from the state should help our citizens, customers, partners, and co-workers. It should be thought-provoking and build a sense of community. If it helps people improve knowledge or skills, build their businesses, do their jobs, solve problems, or understand the state better—then it's adding value.

**Your Responsibility**: What you write is ultimately your responsibility. Participation in social computing on behalf of the state is not a right but an opportunity, so please treat it seriously and with respect. Please also follow the terms and conditions for any third-party sites.

**Be a Leader**. There can be a fine line between healthy debate and incendiary reaction. You do not need to respond to every criticism or barb. Try to frame what you write to invite differing points of view without inflaming others. Topics that are not within the Agencies and State mission should be avoided, such as politics. So be careful and considerate. Once the words are out there, you can't really get them back. And once an inflammatory discussion gets going, it's hard to stop.

**Did you make a mistake**? Admit it. Be upfront and be quick with your correction. If you're posting to a blog, you may choose to modify an earlier post—just make it clear that you have done so.

**If it gives you pause, pause**. If you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit 'send.' Take a minute to review these guidelines, State policy and Agency policy and try to determine what's bothering you, and then fix it. If you're still unsure, you might want to discuss it with your manager. Ultimately, what you publish reflects on your agency, should only represent information your agency wants to represent, and is your responsibility.

**Moderation Guidelines.** Moderation is the act of reviewing and approving content before it's published on the site. While we strongly encourage user participation, there are some guidelines we ask you to follow to keep it safe for everyone. Please have a review procedure in place for inappropriate content.

**Balanced online dialogue.** Before becoming involved with social networking technologies discuss how you will handle the dialogue. A good rule is “the Good, the Bad, but not the Ugly”. If the content is positive or negative and in context to the conversation, then the content is approved , regardless of whether it's favorable or unfavorable to the state. But if the content is ugly, offensive, denigrating and completely out of context, then the content is rejected.

## IV. PROCEDURE REFERENCE

P5040 – USE OF SOCIAL NETWORKING SITES

## V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

## REVISION HISTORY

Effective Date: April 15, 2014