



January, 2011

## Workplace Social Media Policies

PRUSIK USA® LLC

By Justin Oldham  
President/ CEO



PROFESSIONAL SOLUTIONS™

For security consulting and security services information call 1-877-PRUSIKUSA, or E-mail: [securityinfo@prusikusa.com](mailto:securityinfo@prusikusa.com).



Social media policy in the workplace is a hot topic and well it should be. The need to guide employees in proper behavior and procedure online is important. Your social media investigations and vetting applicants on the Internet for cyber-vetting recruits need to be covered by policy as well. This is an overview of some important considerations for all three social media policies.

### I. Communication Policy / General Use

1. **Integrity.** Employees active in social media should be reminded that integrity is the ethical ingredient to using social media. All information disseminated should be absolutely accurate.
2. **Disclaimers.** If you give personnel the authority to comment on issues relating to the organization, emphasize to them to state their posts are their opinion; not the organization's.
3. **Identity.** Organizations should insist that online participation that relate to the organization, or activities/ issues with which the organization is engaged; employees use their accurate identity.
4. **Competence.** Employees should not use any social media tool unless they fully understand how it works. Many of the problems with employees getting themselves into trouble happen on Facebook and often the employee(s) involved indicate they didn't know Facebook worked the way it does. Hold your staff responsible/ accountable for assuring their competence online.
5. **Management responsibility.** Standard disclaimers, do not by themselves, exempt management from any special responsibility. By virtue of their position, they must consider whether personal thoughts they publish may be misunderstood as expressing opinions of the organization.
6. **Training.** Provide social media training for your employees and staff. Once your policy is written, be sure to distribute it with conversations about organizational support for social media.
7. **What's not Okay to post.** This may include things such as organization identification, operations information, or other information that could reflect negatively on the organization.
8. **Implications on career.** All violations of policy or misbehavior online could have detrimental effects on an employee's career. One that doesn't seem obvious to all is the effect simply having a social media profile, even if there's never a problem, could have an effect on an employee's future ability to perform future operations, or participate in special projects.

*An important element for social media policy is that your organization ensures that personnel are all treated equally. Practicing consistency goes hand in hand with saying you do so.*



### II. Cyber-Vetting Policy

#### 1. Notice and Consent

- **Informing applicants.** It's essential to let applicants know that you'll be conducting a search of their social networking profiles. Your policy should state that they will be told and at what point in the process they will be told.
- **Consequences of not giving consent.** Consent needs to be given to search a person's online profiles, especially if the organization expects to search password-protected sites. The applicant should be told that not giving his or her consent could disqualify him or her from consideration.
- **Type of information investigator may collect.** Will it be ok for your agency to speak with the online friends of your applicants? Some organization may object, but is it different from visiting their neighbors? Define circumstances under which organization may contact online friends, inform the candidate, and consistently apply it to all applicants.

#### 2. Quality Assurance & Training

- **Internet search training for investigators.** Online media is complex. Investigators need to understand the nuances of privacy settings, imposter pages, gathering and storing of evidence.
- **How they're monitored.** What procedures are in place to make sure the investigator is operating professionally and securely?
- **Ongoing refresher training.** Because platforms like Facebook changes, so do the rules, and because there are always new platforms of which you need to be aware, make sure the investigator attends training at regular intervals.

*Training and competence are not the same. So provide the training, but include separately that employees will be held accountable – blaming mistakes on not knowing won't be tolerated*



A great way to share files?  
Or a massive security risk?



For more information on Training courses and solutions, call 1-877-PRUSIKUSA, or E-mail: [traininginfo@prusikusa.com](mailto:traininginfo@prusikusa.com).

### III. Investigations Policy

- **False identities.** Give proper consideration for the procedure by which you will obtain false identities and take into consideration the workings of each platform.
- **Organization only equipment.** The use of organization-only equipment which has no online identifiable ties to the agency. This is standard in any investigation but take special consideration for the use of mobile technology, especially geo-location enabled.
- **Training/ Competence.** There's always a new tool, usually a very simple one that will benefit your organization. Keep your investigators well trained and don't underestimate the value of training by professionals. Include in your policy that training is to be provided and investigators need to take on responsibility to know what they don't know and learn it.
- **Proper documentation.** The technique of gathering of anything online should be treated with great care. How it was obtained, with date-stamp, in the chronological order it was obtained is of utmost importance. And, with social networks, the content itself changes quickly. Don't lose sight of the need to document carefully.
- **TOS violations.** Some investigative activity is technically against the Terms of Service for social networking platforms. Know the TOS statements of the platforms you're using and put into policy under what circumstances your organization will conduct activity which may otherwise be in violation of those TOS.

*No matter what you read or who you talk to, always honor the culture of your own organization when developing policy. The organization will benefit because the employees won't feel like it's just not worth doing because it's too easy to get into trouble.*

## Building a Proactive Safety Culture

By John Robishaw  
Health and Safety Coordinator

As the saying goes, "To a little boy with a hammer, everything begins to look like a nail." The same is true of the approaches to improving safety performance. Based on studies by leading expert Don Eckenfelder, behaviorists believe that implementing a behavior-based safety program will improve safety performance. Regulators believe that passing new regulations can improve safety performance.

CEOs look at systems and programs, while engineers want to improve equipment and system designs. All are right to a degree, but if you do them and you have a corporate safety culture that is resistant, it won't work. Some has the tools to help safety managers build a proactive safety culture. Safety culture predicts safety performance. If the safety culture is wrong, safety processes won't work and safety performance won't improve. The way we've dealt with safety culture is unconscious; manage the business and the culture follows. This program allows safety professionals to manage the culture consciously and strategically. We must deal with the safety culture of the organization first, because it is the platform on which the rest of the business is built. This teaches how to measure and manage the safety culture and how it relates to safety and business performance. The Safety Culture Barometer, Exercises for Improvement.

- The Performance Map is a causation diagram. It explains the relationship between culture and performance. Employers should be improving attitude by working on beliefs and values that lead to an organization culture that predicts the attitudes that will exist within an organization. The desired behaviors will then occur naturally.
- The Bridge Metaphor is based on the concept, "If you fall off the bridge for any reason, you are in the water and experiencing undesired losses and the associated costs". The bridge must be strong in all areas, including technology, compliance, systems, programs and culture. Culture is most important, and the best way to make the other areas strongest is to deal with culture directly and so change it consciously and strategically.
- The Safety Culture Barometer is the measurement "tool." The Safety Culture Barometer could be described as a maturity grid. It takes the beliefs and values that are designed to encourage the development of the attributes of safety excellence and establishes organization levels of maturity by collecting data from all employees or a selected cross-section of employees. The data is collected anonymously and leads to the creation of an organization Safety Culture Profile that can be displayed by shifts, departments or levels of the organization or all the above and more. This illustrates where safety culture is weak and where it is strong.

Steps to enrich the safety culture can be taken consciously and strategically. If we need to strengthen ourselves physically or intellectually, we do "exercises." The same thing must be done to enrich culture. After some experience with these processes, organizations can customize the exercises to fit their circumstances.

*After attending Safety Culture Training, CEOs have returned to their companies and changed the safety culture, for the better.*

