

# MANAGE YOUR RISK

## Social Media - Employment Practices Risk Management

Employees are utilizing social media networks and websites at a rapid pace. Facebook, YouTube, Twitter, LinkedIn, personal Web pages, and blogs are only a few of the current social media resources tapped frequently. Employees' usage, written content, as well as photographic and video-based images on their social media sites can create a multitude of problems for them as individuals and the entities they work for.

Your organization may have an interest with employees' social media communications that are considered a breach of confidential information, inappropriate, offensive, unprofessional, disparaging, defamatory, discriminatory, or harassing. Among other risks, an employer could be held liable for its workers' postings on their personal social media networking sites. This bulletin provides analysis and risk management guidelines for managing difficult issues involving social media usage.

### **Employees' reasonable expectation of privacy versus employers' interest in objecting to individuals' personal social media usage:**

An inherent conflict regarding social media is an individual's reasonable expectation of privacy or confidentiality when the content (written text, pictures, or videos) is being disseminated on the World Wide Web. Any person posting a video on YouTube, for example, is essentially the owner of his or her own international Internet distribution center or "television" station. An employee's social media content could be distributed for "the world to see" even when it is not the intention. An email, Facebook post, photograph, blog, or video, could be passed along to an endless number of recipients.

Of course, individuals may attempt to limit who has access to their social media sites or communications, but these communications frequently land in the hands of unintended recipients. Inappropriate, offensive, or personal communications often are called to the attention of the business entity's leaders who are left to determine what actions, if any, could or should be taken against the employees who authored the written content, or posted the pictures or videos.

### **A variety of different factors should be taken into consideration when assessing the employer's interest in objecting to employees' social media usage:**

- **On employer time or within organization facilities** — The organization has a stake in what behavior or activities its employees are engaged in while "on the clock," within organization facilities or otherwise engaged in business-related activities. Employees should be cognizant of their inappropriate usage of business-owned telephones, computers, or other devices to communicate offensive, intimidating, discriminatory, harassing, or other unprofessional social media content. Employees may be disciplined even when using their own personal laptop computer or Smartphone while on duty, organization property or otherwise engaged in business-related activities.

DISCLAIMER: This is a sample guideline furnished to you by VFIS. Your organization should review this guideline and make the necessary modifications to meet your organization's needs. The intent of this guideline is to assist you in reducing exposure to the risk of injury, harm, or damage to personnel, property, and the general public. For additional information on this topic, contact your VFIS Risk Control Representative at (800) 233-1957.

©2019 VFIS. All Rights Reserved.



- **“Off-duty”** — Employees may post pictures, videos, or written text on their personal social media site while off-duty. However, it is crucial employees understand that postings made on their own time, from their own computer or Smartphone, and while off entity property can still harm the organization, its personnel and the community served. Under a variety of circumstances, these off-duty communications can be tied directly to business-related activities, personal or professional reputation within the community or co-worker relationships.
- **Business-related information** — Employees may use their personal social media networks to discuss business-related information and could violate confidentiality laws and/or business policies. Workers may communicate sensitive or confidential information about the organization’s financial, operational and personnel functions.
- **Co-workers as subjects of postings** — Problems result when an employee posts information, allegations, pictures, or videos about co-workers that could be considered harmful to that individual. For instance, an employee can post disparaging allegations that are harassing, discriminatory, or retaliatory in nature against co-workers. Again, it may be considered irrelevant if the offending party posts such information while on or off-duty.


## Policy Development

Work with locally retained labor and employment counsel to develop policy language pertaining to employees’ usage of social media. Personnel decisions such as hiring/selection, discipline, terminations, demotions and promotions can be impacted by employees’ social media usage. Legislation and case law is ever changing in part due to new social media technologies. Legal concerns may include non-union employees’ rights to engage in “concerted activities” as protected by the National Labor Relations Act, whistleblower protections, some states’ laws protecting “legal off-duty activities,” and wrongful termination and discrimination claims.

An employer may develop a stand-alone policy addressing social media or networking. Alternatively, policy language specific to social media can be woven into an existing entity policy on other electronic communications systems. Remember that there are likely policies already in place within your entity that could be applied to social media usage, such as policies that address:

- **Breach of confidentiality or unauthorized communications regarding private business-related information** — This may include financial data, operational, medical, sensitive personnel relations matters or even photos or videos taken at business-related events.
- **Inappropriate usage of business time or equipment (i.e. computers) or is otherwise detrimental to productivity, morale, work culture or mission and purpose of the entity** — Social networking has been referred to as social “not-working” because so many employees are spending work-related time on their personal social media sites.
- **Code of Conduct** — Many organizations institute policies that allow employees to be disciplined for behavior on or off-duty that reflects poorly on the integrity and professionalism of the entity.
- **Misuse or misrepresentation of the entity’s name or business** — For their personal social media site, employees may “copy and paste” the entity’s logo and consequently violate copyright or trademark laws or protections.
- **“Representing” the employer or entity** — An individual’s social media site may indicate he or she is an employee of a certain business entity. Therefore, representations made by that person on the social Web site could be misperceived as representing the views of the entity.
- **Harassment, discrimination, retaliation or other behavior that may be considered inappropriate, offensive, or intimidating.**





Personnel should receive and sign a form acknowledging their understanding of the parameters of the electronic communications systems (including social media) policy. The form also should include the entity's ability to monitor their usage while on duty, within organization facilities or while engaging in business-related activities.

Implementing a policy that bans employees' usage of social media networks is most likely unrealistic and will be perceived as overreaching by personnel. Instead, focus on a policy that is grounded in common sense and places reasonable restrictions on content and usage.

### **Train, Train, and Train Some More**

Utilization of social media and other electronic communications systems is complicated and a daily-changing subject matter. Attempting to adequately address the topics by written policy alone is not recommended. Employers are encouraged to provide training for its personnel on social networking and other electronic communications systems. It is important to not only explain the parameters of a social media and electronic communications systems policy, but also allow for questions. Straightforward, periodic training will help personnel understand that the employer is not trying to play "big brother," but instead regulate social media usage that may be clearly detrimental to the entity or its workers.

### **Conclusion**

Americans value and protect their reasonable expectations of privacy in respect to their personal activities, such as what Web sites they frequent, communications they author or photographs or emails they send. However, problems often arise when a worker's personal communications are inappropriate, offensive, disparaging, or discriminatory and disseminated to others within the entity or members of the community served.

It is clear that as individuals we choose how to communicate with others. Social media carries a greater risk of information being distributed to many outside the originally intended scope of communication. Educate employees about exercising sound judgment when utilizing social media, while reinforcing the potentially detrimental impact of irresponsible communications.