10 Social Media Commandments for Employers

Social media networking is a fact of life for millions of people, so the question is how far employers can and should go to guide employees' social networking activities while on the job.

Here are 10 social networking commandments for employers. If followed, they will enable employees to enjoy social media without employer static and interference:

1. Develop a policy. Influence appropriate work-connected behavior and use with a social media or networking policy. Privacy rights are gaining ground, but employers have rights too, to create and enforce reasonable policies to protect employees, property and reputation, by framing acceptable and unacceptable e-behavior.
2. Use your social media policy to set employee boundaries. Employees need practical guidelines to help prevent unthinking or harmful activities. Employees need to be told, nicely but firmly, what you expect from them.
3. Echo important employment considerations in your social media policy. Assure employees that social networking can be wonderfully fulfilling, but thoughtlessly using the Internet for social networking can cause serious harm to the company and our jobs. We must avoid:

   • Illegal activity.

   • Disclosing trade secrets or other confidential or sensitive information.

   • "Watering down" patented or copyright-protected information.

   • Harassing or otherwise spreading gossip—or even confidential truth—about others.

   • Wasting our work time or that of others.
4. Monitoring is crucial, but so is employee consent. Monitoring should be a non-issue. Ignorance is not bliss and it's certainly no legal defense.

   Monitoring employee use of social media without clear consent is risky. Employees can agree to and accept as reasonable the privacy standards that employers offer at the time of hire, or as a requirement for continued employment. It's not necessary for employees to consent in writing to privacy expectations. But written consent – ideally in a letter offering employment - is easier to obtain and prove in case of a dispute.

   Implied consent for existing employees is the norm. It typically starts with an electronically and physically posted message to employees, announcing a change on a specific date for all employees. Employees who continue working after the effective date of the change have implied their consent.

   Even with consent, overbroad or intrusive monitoring can cause trouble. Communication is always helpful. Before seeking consent:

   • Provide examples of valuable, acceptable use of social media.

   • Use stories of how new Internet "friends" are not always who they say they are.

   • Specify, with concrete examples, acceptable and unacceptable social networking.

- Ask employees to reverse roles: "Imagine if an employee said this about you."
- Specify simple guidelines and require employees to meet them. Only then should you seek consent.

5. Decide how to monitor in the least intrusive way to seek needed information. Overly intrusive methods can offend employees, courts and juries.
6. Seek only necessary work-related information. An employer's right to monitor and search extends only to information needed to protect its business and its people. Never seek other information.
7. Be yourself. Never pretend to be someone or something else to access and get information from a site. Serious legal consequesces can arise by pretending to be an employee and using his/her password.
8. Know and obey applicable law. "Ignorance of the law is no excuse." Keep abreast of all possible laws that apply to monitoring and do not stretch the envelope.
9. Act to protect. Discovery of dangerous or damaging information on a site demands immediate and effective action tailored to the particular facts. That typically means requesting that the site remove the offensive information.

   If that effort fails, however, approach the offending employee, if that person can be identified, and persuade him or her to remove the posting by offering lesser discipline for cooperation.

   It is also important to investigate who is at fault and, if it was an employee, what action is appropriate.
10. Be actively vigilent. Remain diligent, aware and safe and secure in protecting your business, your fine reputation, your employees and their morale.

Social media networking is a reality. Maintaining and enforcing an effective social media policy, monitoring sites that your employees frequent and enforcing your policy when necessary are musts for survival in an electronic arena where a thoughtless, reckless or vicious electronic rumor can doom a business.

This is an edited version of an article by Gene Connors from Workforce Management Online

118 Charnwood • Beaconsfield (QC) • H9W 4Z3
Phone: (514)-573-3012 • e-mail: mhiles@total.net