# Social Media in the Workplace- Why Employers Should be "Linked In"

Consider this - *Twitter* reports more than 175 million registered users posting more than 95 million tweets per day; *Facebook* reports more than 500 million active users spending more than 700 billion minutes per month on the site; and *YouTube* reports more than 2 billion videos are viewed each and every day. Against this backdrop, ask yourself, *'What are my employees posting about me, my managers, our clients and our company in general?".* In today's digital landscape, protecting your company brand and reputation has presented new challenges in the workplace.

**Don't put your head in the sand**

When the social networking phenomenon began, many employers dealt with it by not dealing with it - they simply banned/blocked social networking sites on the company network. That didn't work so well.

Today's generation of young workers have grown up with Internet access and come to the job with the expectation they'll have those resources at their disposal. If you deny them the ability to check their Facebook pages during lunchtime or tweet when they're taking a coffee break, they'll find a way around it or leave to work for a company that has fewer restrictions.

But it's not just about catering to a new technologically-savvy generation of workers. Businesses are learning that social networking, used properly, can be an effective business tool. Having your employees involved in the community can enhance the company's reputation and bring in more business - so long as it's done right.

Even so, you still need to exert some control over how these sites are used. You can't just give employees free rein and hope they'll all exercise common sense. And you can't, in all fairness, blame them for violating rules that don't officially exist. You need a social networking policy that explicitly lays out what is and isn't permissible, both on the company's network and outside of it if they're presenting themselves as representatives of the company.

If you do decide to take the "easy" way out and just block social networking sites at the company firewall, remember that what employees are posting from home can still affect your company's reputation. The view held by some posters that employees have a reasonable expectation of privacy and cannot be disciplined for their actions outside of the workplace is simply not true. More and more, employees are faced with the reality that since Internet sites are public in nature, anything posted on the Internet can and will be viewed by their employer or prospective employers.

**Adjudicators have been slow to catch up...**

Canadian adjudicators are just beginning to dip their toes into these uncharted waters. However, it is becoming increasingly clear that the difference between 'annoying' posts and ones worthy of workplace discipline comes down to whether an employee's online posting directly affects the employer's business.

In *Lougheed Imports Ltd. (c.o.b. West Coast Mazda) v. United Food and Commercial Workers International Union, Local 1518* the British Columbia Labour Relations Board recently upheld the dismissal of two employees who posted disparaging remarks about their employer on *Facebook*. Collectively, the employees had 500 *Facebook* friends, including colleagues and supervisors. The postings against the employer and managerial staff were of a threatening and homophobic nature and discouraged customers from doing business with the company. When asked about the posting during a disciplinary investigation, the two employees were dishonest and denied their conduct. The Labour Board found the postings were damaging to the employer's reputation and degraded managerial staff.

**An employer's best defence is a good offence**

The old adage that the "best defence is a good offence" is applicable here. Employers should set the boundaries of employees' online conduct in a written social media policy which should include at least the following:

**1. A clear workplace philosophy**

Before you can develop a policy, you need to define the workplace's overall attitude toward social networking. Is it something you consider to be a strictly personal activity, which should be generally restricted to the employee's break and lunch times? Or is the workplace interested in encouraging employees to use social networking for business purposes and incorporate it into their working time?

Some sites, such as *MySpace*, are primarily for personal socializing. Some, such as *LinkedIn*, are purely for business. But others, such as *Facebook* and *Twitter*, straddle the fence and are used by many for both purposes. You may want to allow or disallow use of specific sites during work time, but that's a challenge because new sites are always popping up and old sites are always evolving. For example, *Facebook* began as a venue for college students, but the demographics have changed.

**2. The definition of "social networking"**

It's important that your policy define what is meant by "social networking" or "social media," since the term means different things to different people. Everyone knows *Facebook* is a social networking site, but what about *Flickr* (photo-sharing site), or *LiveJournal* (blogging site)? Are web forums, such as those hosted by many workplaces for their customers to ask questions, considered a form of social networking under your policy? What about "old-fashioned" online networking methods, such as email discussion lists and newsgroups?

**3. Identifying oneself as an employee of the company**

Your social networking policy should make clear whether employees are allowed to identify themselves as representatives of the company. Most social networking sites have fields in the user profile for work experience, job title, etc. By identifying oneself as an employee of XYZ Inc., a social networker becomes, to some extent, a representative of that company, and everything he/she posts has the potential to reflect on the company and its image. Unless the employee is engaging in social networking for the specific purpose of promoting the company, some organizations prohibit their employees from listing the company name on such sites. If employees are allowed to advertise their association with the company, your policy should impress upon them that they take on the responsibility for representing the company in a professional manner.

If social networking users identify themselves as employees of the company, your policies should require that any personal blogs and other personal posts contain disclaimers that make it clear that the opinions expressed are solely those of the author and do not represent the views of the company.

**4. Recommending others**

Some social sites provide for members to write recommendations or referrals for friends/associates. If an employee does this as a representative of the company, it may give the appearance the company endorses the individual being recommended. For that reason, some company policies prohibit employees from making recommendations or referrals.

**5. Referring to clients, customers, or partners**

Your company's relationships with clients, customers and partners are valuable assets that can be damaged by a thoughtless comment. Your social networking policy should make it clear that employees are not to reference any clients, customers, or partners without obtaining the company's express permission to do so (and the company should in turn receive prior consent from the client, customer or partner).

**6. Proprietary or confidential information**

Even though you may have other policies that cover the dissemination of the company's proprietary or confidential information, trade secrets, etc., the social networking policy should reiterate those policies and

provide specific examples as they relate to social networking sites. Because social networking communications are somewhat informal, it's easy for employees to let their guard down - especially when they think they are discussing only among themselves.

Social networking sites have varying levels of security and as public sites all are vulnerable to security breaches. Your policy should make it clear that proprietary information is not to be discussed or referred to on such sites, even in private messages between site members who have authorized access to the information. You may want to spell out examples of information that is considered to be off limits, such as the company's (or an individual's) financial, personal or legal information, intellectual property, information about customers, and so forth.

**7. Terms of Service**

Most social networking sites require that users, when they sign up, agree to abide by a Terms of Service document. Your policy should hold employees responsible for reading, knowing, and complying with the Terms of Service of the sites they use. It should not contain rules that require employees to violate the Terms of Service. For example, most Terms of Service agreements prohibit users from giving false names or other false information, so the company policy should not require users to use pseudonyms when signing up for social networking sites.

**8. Copyright and other legal issues**

Policies should require that employees at all times comply with the law in regard to copyright/plagiarism. Other relevant laws include those related to libel and defamation of character.

**9. Productivity impact**

Social networking sites can be good tools for developing business relationships, but they can also turn into big time-wasters. It's easy to set rules for purely personal use of the sites, but it's more difficult to draw the lines when it comes to business-related networking. Your policies should make it clear that social networking activities are not to interfere with the employee's primary job responsibilities.

**10. Disciplinary action**

To have teeth, a policy must include consequences for violations. The policy should spell out that a violation can result in disciplinary action, up to and including termination for cause.

**Pam Shin and Farrah Sunderani are lawyers with Sherrard Kuzz LLP a management-side employment and labour law firm in Toronto. Pam and Farrah can be reached at 416.603.0700 (Main), 416.420.0738 (24 Hour) or by visiting http://www.sherrardkuzz.com/ .**