3 steps to rein in social media misuse in the workplace
by Curtis Armstrong
March 5, 2014

he Internet and social media have changed our world. Communications, which 20 years ago took days if not weeks to make their way throughout a workplace, now take mere seconds to reach tens, hundreds, and even millions of people around the world. Theoretically, this unprecedented access to information should mean we are better-informed and more productive than we were in any previous generation. But are we?

Employers and practice owners know that not every aspect of this new technology is positive. Studies suggest access to the Internet during business hours can reduce workplace productivity by up to 40 per cent, as employees turn their minds from work to social interaction and play. Workplace bullying and harassment is also on the rise, due in part to the ability of colleagues to reach each other secretly via the Internet, rather than publically by the water-cooler. The anonymity of the Internet has also enabled many a malevolent blogger and tweeter – often an employee – to destroy products, brands and entire organizations.

Fortunately, much of this behaviour can be minimized when employees understand the parameters and consequences of Internet misconduct. To this end, we can divide Internet misconduct into two categories:

1. Misconduct while on the job (e.g., excessive personal use of the Internet and/or accessing prohibited sites during work hours, etc.); and
2. Misconduct that may take place outside of the workplace (e.g., offensive, irresponsible, defamatory blogging, Tweeting, harassment, etc.).

The first form of employee Internet misconduct is the easier of the two to identify and discipline. Relatively simple technology allows employers to track time spent online, sites accessed and content downloaded and/or uploaded. If misconduct is identified, it can and should be dealt with appropriately.

The second form of misconduct can be more problematic. Canadian courts and labour arbitrators have traditionally drawn a line between an employee's work and private life, declining to uphold discipline for "off-duty" conduct where there is no clear connection to the workplace. In some cases that connection is obvious – for example, where the company is criticized publicly. In other cases, the line is not as clear.

Consider the case of the tragic death of high school student Amanda Todd. In the aftermath of her suicide following relentless bullying and harassment, an employee of a retail store in Ontario, a man with no apparent connection to Ms. Todd, posted to Facebook the comment: "Thank God this b---- is dead." A Calgary woman tracking Facebook comments about Ms. Todd saw the posting, and when she viewed the poster's online profile saw the name of his employer. She reported the posting to the employer who immediately fired the man because the posting was contrary to the employer's values and the poster could be publicly identified as its employee.

Was the man's posting sufficiently connected to the workplace to justify his termination? We may never know, as the case has not been adjudicated. It is, however, a thought-provoking example of how online comments, even ones not directly related to the workplace, can have a workplace impact.

Here are some steps that can be taken to minimize the risk to business caused by employee misuse of technology and social media.

Step 1: Have an Internet use and social media policy
A clear, direct Internet and social media policy is essential as a means of communicating to employees the limits of acceptable online communication and conduct. When and how to introduce a policy into the employment relationship (or amend an existing policy), depends on several factors which should be discussed with experienced employment counsel.

At the very least, an effective Internet use and social media policy should outline permitted and prohibited uses of workplace technology and social media. This includes advising or reminding employees of the following.

- They should have no expectation of privacy as it relates to the use of company technology
- The employer has the right to monitor computer usage within and about the workplace
- The employer monitors social networking sites (if accurate)
- The limits to Internet use during work time (total prohibition is rarely reasonable or practical)
- That online communications may be seen by anyone (including the employer, co-workers and members of the public)
- The prohibition on publishing negative comments, not only about the employer, other employees or customers, but any comments that may negatively affect the employer's reputation (e.g., defamatory, offensive, threatening, harassing, etc.)
- The prohibition on disclosing confidential information about the company, employees or customers
- Applicable, companion policies, such as harassment, confidentiality, conflicts of interest and privacy
- The process for addressing complaints
- That violation of the policy may result in discipline, up to and including termination for cause

Step 2: Monitor usage
An employee who believes Internet misconduct cannot be seen has less of an incentive to behave, which is why monitoring Internet and social media use inside and outside of the workplace is the second essential step.

Inside the workplace requires the implementation of technology that has been available for years, and is not expensive. This technology can track time spent online, sites accessed and content downloaded and/or uploaded (e.g. confidential company information, or personal customer or employee information).

Outside the workplace provides the ability to monitor public social media communications around the world, identifying those which fit a profile the employer determines it wants/needs to track. For example an employer may determine it should be alerted every time the organization's name is mentioned in a public Tweet, blog or social media forum.

In both cases, whether tracking activity from within or without the organization, it is important to implement methods that are the least intrusive necessary to achieve reasonable business ends.

Step 3: Implement and enforce

Even the best written policy is of little significance if not implemented properly. In our experience, a well-implemented policy has four key components:

Relevance: Management and employees should be educated on how and why the policy is relevant to and will apply to their day-to-day responsibilities.

Proportionality: The impact of the policy must be reasonable and rational; neither overreaching nor attempting to attain a 'gold standard' that may not be necessary.

Consistency: The policy must be applied consistently and fairly so as not to lose credibility within the workplace.

Flexibility: The policy must be a living document, able to adapt to and reflect the organization's business realities as they may change from time to time.

For better or for worse, the Internet and social media have become a workplace reality. The objective for employers is to harness the benefits of this exciting technology, while at the same time protect the business from its dangers. This can be accomplished by having a clear and unambiguous Internet and social media policy, monitoring internet and social media usage as it relates to the workplace, and enforcing the Internet and social media policy consistently and fairly.

Curtis Armstrong is a lawyer with Sherrard Kuzz LLP, Toronto-based employment and labour law firm representing the interests of employers. Curtis can be reached at 416.603.0700 (Main), 416.420.0738 (24 Hour) or by visiting www.sherrardkuzz.com.

The information contained in this article is provided for general information purposes only and does not constitute legal or other professional advice. Reading this article does not create a lawyer-client relationship. Readers are advised to seek specific legal advice from Sherrard Kuzz LLP (or other legal counsel) in relation to any decision or course of action contemplated.