

CANADIAN Employment Law Today

Reigning in employee misuse of Internet and social media

Curtis Armstrong

November 13, 2013



Policing online activity

The extent to which people are connected with each other through the Internet and social media is so pervasive that often people find it strange if they're off the grid. Many employees are connected at work, whether through company equipment or their own, and they continue to be after work as well. But with little regulation, people can do whatever they want online, which can be a problem if they're identified as employees.

While it's not easy to keep track of and regulate employee activity on online, employer's can take steps to mitigate the risk of legal liability or damage to their reputations. Employment lawyer Curtis Armstrong discusses reigning in employee abuse of the Internet and social media.

The Internet and social media have changed our world. Communications which 20 years ago took days, if not weeks, to make their way through 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 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. And the anonymity of the Internet has enabled many a malevolent blogger and tweeter — often an employee — to destroy products, brands, and entire companies.

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:

- Misconduct while on the job (for example, excessive personal use of the Internet and accessing prohibited sites during work hours)
- Misconduct that may take place outside of the workplace (such as offensive, irresponsible, defamatory blogging, tweeting and harassment).

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 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 publically. 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 Todd, posted to Facebook the comment: "Thank God this b---- is dead." A Calgary woman tracking Facebook comments about Todd saw the posting, and when she viewed the poster's on-line 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.

Steps to minimize misuse of technology

What then are the steps that can be taken to minimize the risk to business caused by employee misuse of technology and social media?

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)
- 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 (defamatory, offensive, threatening or harassing)

- 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
- Violation of the policy may result in discipline, up to and including termination for cause.

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 uploaded (such as confidential company information and 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 or 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 as necessary to achieve reasonable business ends.

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.

Final thoughts

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.