How to Regulate Employee Social Networking Activity – Both On-and Off-Duty

This is an article from 2020, reflective upon the COVID-19 pandemic, but the principles and strategies mentioned are still applicable for HR directors who want to regulate and understand employee social media use.

The things employees say on social networks can do serious harm to your business.

What's At Stake: The Damage Employees Can Do on Social Media

On November 27, with the state of Oregon reeling from a record surge of new COVID cases, something almost equally virulent went viral, namely a video posted on TikTok by a hospital oncology nurse mocking the public health restrictions. Bedecked in scrubs and stethoscope, Ashley Grames boasted about not wearing a mask in public and letting her kids have play dates. Ms. Grames was placed on leave and agreed to give up nursing, but the damage was done, with the scandalous video attracting hundreds of thousands of views from across the country.

The Ashley Grames fiasco is in some ways the literal face of why employees' social media activity is legitimate grounds for workplace discipline, even when it occurs when they're off-duty. While employers have been grappling with regulating employee social media conduct for more than a decade, the COVID pandemic has infused the challenge with a new urgency. The good news is that the legal parameters for disciplinary action against employees for social media activity, whether on- or off-duty, have become fairly clear. Here's what HR directors need to know.

It's YOUR Business

The starting point is to recognize that social networking by employees isn't purely a private matter. Over the past decades, courts and arbitrators have consistently recognized that blogging, tweeting, Facebooking and other forms of social media activity is NOT harmless, but has real and meaningful impact on employers, and their staff, reputation and business. Accordingly, the first challenge employers face is in a disciplinary proceeding is to demonstrate how an employee's social media activity harmed the organization. While cases differ, the cases recognize 7 basic kinds of threat and harm:

1. Productivity Losses

Anyone who has at least dabbled in the experience of social networking and other Internet activities like web surfing, shopping, downloading family photos or just catching up on the baseball box scores, can understand just how addictive these activities can be and how easily they can suck up your time. Thus, what may be intended as a simple exchange can suddenly turn into a day-long interaction that soaks up the time and energy that employees should be dedicating to their jobs.

How serious is this problem? Studies done before the pandemic suggest that social media and internet use productivity losses are costing Canadian businesses billions of dollars per year. For example, one study revealed that Canadian adults who have Internet access at work spend an average of 4.5 hours a week online for personal reasons—a total of 1.6 billion hours per 50-week work year for all Canadians! A BBC report cites a recent study that reveals that social networking could be costing UK employers an average of about £130 million in lost productivity—per day!

2. Threats to Business Confidentiality

One of the things people like to talk about online is their jobs. And in a social context, they tend to speak candidly. When such conversations occur face-to-face or on the phone, they're generally kept private. But keeping such interactions private is much more problematic when they occur online, especially within an external service network (ESN) like Facebook or Instagram. Just about anybody who has access to the internet can join an ESN and get in on the conversation.

One of the most serious risks is that employees will reveal confidential or compromising information about the company or the business. For example, the employee might express concern to her Facebook chum that her company is talking to another corporation about selling off the business unit she works for. The disclosure may not be a deliberate attempt to disclose a company secret. The employee may simply not know that the negotiations with the other company are top secret. But even if the indiscretion isn't ill-intentioned, once the information is out in cyberspace, the damage is done.

3. Undermining of Management

Complaining to friends about work, bosses and colleagues is a venerable and largely harmless social tradition. But when it happens online, it's much more serious, even if the whole conversation takes place while the employee is off duty and at home. In a cyber world, gripes get expressed in the form of inappropriate postings, pictures and jokes about bosses and co-workers on the internet where anybody can see them. In addition to harming morale and collegiality, such communications can expose the company to the risk of liability for harassment, discrimination and other violations. They also can be a form of insubordination or insolence to the extent the communications are contrary to explicit company policies or undermine managerial authority.

Example: In her blog, an Alberta employee referred to the nurse who supervised her as "Nurse Rached"—the nurse from hell in *One Flew Over the Cuckoo's Nest*. Although the employee didn't use her name in the blog, she didn't bother to hide the fact that she worked as a nurse in a hospital department in a particular Alberta community that had only one hospital. Result: It was pretty easy to figure out the identity of the blogger and the supervisor the "Nurse Rached" comment was directed at. An arbitration board ruled that the hospital had just cause to fire the employee for insubordination [*Alberta v. Alberta Union of Provincial Employees (R. Grievance*)].

4. Harm to Reputation

The negative things employees say on social networks and blogs can undo the millions of dollars some companies invest to improve their corporate image and public relations. Just ask the Oregon hospital that experienced a flood of negative publicity and outraged calls from patients and family members after nurse nurse Ashley Grames' notorious TikTok video went viral.

5. Discrimination & Harassment of Other Employees

Employees don't only talk about their bosses and employers in their blogs or social network posts; they also talk about their co-workers. Comments made about co-workers in an employee's blog could constitute harassment or discrimination and expose your company to liability. For example, an employee may make inappropriate sexual comments about or use a racial epithet to describe a co-worker.

Employees may also download, view or transmit pornographic, racist and other offensive material from the Internet at work in violation of your company's harassment or discrimination policies and may expose your company to liability. For example, there are plenty of cases where employees sent objectionable pornographic material to a colleague. And, of course, simply working in a cubicle next to a co-worker who views porn or exchanges smut with co-workers can be extremely offensive.

6. Liability for Illegal Activities

Employees may conduct illegal activity on the Internet at work, such as distributing child pornography or downloading material in violation of copyright law. And there's an argument that your company may be liable for such activities because the employee used your computer and network in your workplace to conduct them. **Explanation:** Prosecutors may argue that your company, by providing the opportunity and the means to engage in illegal activity, condoned it and so is "vicariously liable" for it. That argument is particularly compelling if you knew about the employee's activities and did nothing to stop them.

7. Harm to IT Infrastructure

Employees who use the Internet for unauthorized purposes often introduce viruses, worms, Trojan horses and the like into the company's information network, causing serious problems for the IT infrastructure. Use of the company network for personal business—especially when many employees do it at the same time or when an employee downloads a large file—can also slow down the system and make it harder for other employees to use the network to do their jobs.

3 Ways to Prevent Social Media Abuses

Implement clear and specific policies to establish your right to discipline employees for social network abuses or, better yet, deter them from committing them in the first place. Three strategies that have proven effective:

Strategy 1. Address Social Networking in Confidentiality Agreements

Like many employers, you may ask employees to sign confidentiality agreements banning them from disclosing confidential information. Add language to the agreement requiring employees to abide by their confidentiality obligations while engaging in social networking and other forms of online activity. Spell out that revealing sensitive organization information on an online social network at home is just as

unacceptable as doing it in a business communication during work.

Strategy 2. Address Social Media Use in Codes of Conduct

Most organizations have HR policies or standards of conduct banning unacceptable behaviour like harassment, bullying and bad-mouthing bosses, clients and the organization. Indicate that these forms of misconduct are equally unacceptable and subject to discipline on a social network or other online activity, whether on- or off-duty.

Strategy 3. Set Specific Policy on Employee Social Networking

The centerpiece of your effort to curb social media abuses is to establish and consistently to enforce an employee social networking policy that addresses these activities. Make sure your policy is realistic. Simply banning employees from using social networking sites or blogging altogether is impossible to enforce, especially to the extent it applies to what employees do off-duty. Spell out that:

- All company computers, IT equipment and Internet access is intended for business use only and may not be used for non-work-related purposes;
- Employees are expected to work while on duty;
- Employees may not post or say anything on a social networking site that harms the company's reputation and good standing in the community;
- Employees may not insult, offend or demean the company or its staff, clients or customers or divulge confidential information about them online; and
- The content of any employee postings must comply with all company HR policies, including its code of conduct and discrimination and harassment policies.