

Computer – Internet – Social Media Quiz



QUESTION

Whatever an employee does his or her own time after leaving the workplace with respect to his or her own social media platform use and using a personal account is legal and does not have any relevance or affect to employment issues.

Yes or No.

ANSWER

Everything posted in social media like Facebook or Twitter is considered public even if it is just between friends. The content maybe subject to discipline for comments that appear to affect your ability to do your job or that disparage or demean your employer or colleagues.

WHY IS IT RIGHT

What is social media?

Social media such as Facebook, Twitter Instagram and LinkedIn, are Internet-based services that provide individuals a way to interact with each other online. Some organizations may allow employees to access and use their personal social media accounts in the workplace during normal work hours or break-times. Other organizations might develop their own, internal social media to help employees work collaboratively – regardless of their physical location. Some organizations may establish official, external social media accounts to communicate with customers, business partners or the media.

When creating a social media policy, there is no one-size-fits-all plan. Some companies use social media to brand themselves and expand market research, whereas others are simply trying to protect themselves from potential legal and security risks and control employee productivity. Regardless of the type of policy implemented, it is essential that the policy be well understood by employers and employees alike. **Here are some tips on how to create an effective social media policy:**

1. **Consult Broadly:** When drafting a social media policy, it is important to involve all departments. Information technology, human resources, public relations/marketing and corporate managers and executives should all work

together to create a policy that works for everyone.

2. **Consider Scope:** Social media policies should be broad enough to cover social media technology that will be introduced in the future. Furthermore, the policy should not only cover the material on the company blog, or company Facebook or Twitter account, but should cover the appropriate use of one's personal blog, Facebook page, or Twitter account. It must also be clear that the policy is not restricted to use from work computers and applies to use of social networking sites on employee time.
3. **Strike a Balance:** Implement a positive social media policy. This will empower employees rather than leave them feeling restricted. Recognizing the pervasiveness of new technologies, allowing access to social media in moderation could be the answer so long as it does not affect productivity and the company is protected. Perhaps limiting access to specific sites or limiting social networking to the hours before work, after and during lunchtime might work for some employers.
4. **Inform Colleagues:** Educate employees on the legal and security risks involved in social networking and what they can do to protect themselves and the company. Emphasize the need to use caution and good judgment as comments posted on social networking sites can spread despite the original posting being removed. It is important to encourage employees, if mentioning the company name, to use a disclaimer that the opinions expressed are not those of the company.
5. **Specify Acceptable Use:** Clearly define what is and is not considered "acceptable use" both on the company's network and outside of it. It should be clear that company systems may not be used for illegal activity such as copyright/plagiarism and downloading pirated software.
6. **Address Consequences:** The policy and its enforcement should be clear to all employees. It is important to clarify what disciplinary action will be taken, up to and including termination, if policies are not followed.
7. **Document:** A social media policy should be written and it is a good idea to have employees sign off on it or track acceptance or receipt to ensure they have read its contents.
8. **Accessibility:** The policy should be simple and accessible. Employees will not be inclined to read through an overwhelming manual. Circulating the policy regularly and having the policy readily available both electronically and in hard copy is also suggested.
9. **Ongoing Review:** Create a long-term plan for your company and include social media goals. This means re-evaluating your company's position every six months or so. This will enable your company to adapt to advancements in social networking.

With social networking sites becoming more prevalent as a forum of social interaction, the need for a social media policy cannot be understated. It is a delicate balance between restricting the employee's right to freedom of expression and protecting the employer. Employees are entitled to their opinions; however, displaying such opinions may negatively impact the employment relationship and the organization. Social media policies need to be clear that maligning the company or giving up trade secrets is subject to serious discipline. The employer must also be concerned about vicarious liability and ensuring that the views of an employee are not mistaken for the views of their employer. It remains to be seen whether the emerging case law will change the workplace, social media use, or both. However, one thing is certain, companies that maintain an open dialogue with their employees about social networking are those that will be more likely successful in this marketplace.

Jurisdiction

In Canada, **The Privacy Act** deals with the collection, use and disclosure of personal information (including employee information) in the federal public sector. Both the OPC and Treasury Board Secretariat have produced guidance that may be helpful to understanding the use of social media in the workplace. Every province and territory has some form of public sector privacy legislation and an oversight authority.

The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's private sector privacy legislation. In the employment context, **PIPEDA** only applies to federal works, undertaking or businesses (FWUBs) in respect of their treatment of personal information of employees and applicants for employment with FWUBs.

WHY IS EVERYTHING ELSE WRONG

A. PRIVACY IMPLICATIONS FOR EMPLOYEES IN THE WORKPLACE

The use of social media in the workplace raises privacy implications for both employees and employers. Organizations should develop policies on the appropriate use of social media in the workplace.

Most individuals view their personal social media pages as private. However, employees should be aware that any of the information or communications posted on their social media can potentially be accessed by:

- current or potential employers;
- recruitment agencies;
- co-workers;
- the employer's competitors;
- government and law enforcement agencies;
- others outside the employee's trusted network.

Depending on the privacy settings set by the individual user, personal information and communications posted on a social media site can be read by unintended people.

B. MONITORING EMPLOYEE SOCIAL MEDIA

- **Employees should know** that, subject to existing workplace policies and rules, some organizations monitor their employees' social media.
- **Employees should be aware** that when using social media in a workplace context – including a social media account hosted by their employer – that their personal information can be collected, used and disclosed by the employer. This could include off-duty comments and postings on social media about workplace issues or that may otherwise reflect on the employer.
- **Employers should view** tracking existing employees through personal or work-based social media as a collection of personal information that may be subject to applicable privacy legislation in their jurisdiction.

C. STAFFING AND RECRUITMENT IMPLICATIONS

Many employers and recruitment agencies use Internet search engines and read personal social media, websites and blogs to learn more about job applicants –

and existing employees. During the staffing process, this practice may become a problem if it substitutes for more formal and thorough reference checks.

- **Employees should know** that social media information may seem transitory and informal, but once personal information is posted online it gains permanence – and can be circulated and searched by others.
- **Employers and recruiters should be aware** that social media pages, even if publicly available, can contain inaccurate, distorted or out of date personal information about job applicants, and should therefore be cautious about relying on that information.
- **Employers and recruiters should also guard against** using personal information gathered from social media – or any other online source – in a discriminatory manner against a job candidate or an existing employee.

D. INAPPROPRIATE DISCLOSURE ON SOCIAL MEDIA – CONSEQUENCES

Employers and employees should be aware of the potential damages to individuals and the corporation through inappropriate disclosures of personal or confidential business information on social media. The possible consequences of an improper or unintended disclosure may be:

- a defamation lawsuit;
- copyright, patent or trademark infringement claims,
- a privacy or human rights complaint;
- a workplace grievance under a collective agreement or unfair labour practice complaint;
- criminal charges with respect to obscene or hate materials;
- damage to the employer's reputation and business interests.

Legal responsibility for damages from an inappropriate disclosure could potentially rest with individual employees, management or the organization as a whole.

- whether the organization permits the use of personal or employer-hosted social media in the workplace;
- if social media accounts are permissible, in what context and for what purposes may they be used?
- whether the employer monitors social media sites;
- what legislation applies to the collection, use or disclosure of personal information in the workplace;
- what other rules may apply to the use of social media in the workplace (collective agreements; other relevant legislation);
- the consequences of non-compliance with the policy and,
- any other existing policies about the proper use of electronic networks with respect to employee privacy and handling confidential information.

E. WHAT DATA NOT TO INCLUDE

Employers should inform employees in plain language why it's important to keep some personal and corporate information – about themselves, their co-workers, clients and the organization – confidential or undisclosed. Similarly, employers need to exercise judgment and abide by applicable privacy and other legislation if they decide to collect, use or disclose personal information from social media sources. A privacy-friendly workplace calls for fair use of information by all parties.

F. GUIDELINES FOR PERSONAL USE OF SOCIAL MEDIA

Employees have obligations to employees that don't always end when you leave the workplace.

Here are some things to remember when you post to your favorite social media platform, even if you're in the privacy of your home, on your own time, and using your personal account:

- Don't badmouth your employer or colleagues. The B.C. Labour Relations Board found that the "walled garden" of Facebook is not private. Everything you post on Facebook or Twitter is considered public, even if it's just between friends, and you may be subject to discipline for comments that appear to affect your ability to do your job or that disparage your employer or a colleague. Best not even to joke about it: the Internet is the place irony goes to die.
- Avoid being Facebook "friends" with your boss. You're not friends, you're in a power relationship. It's not necessary or advisable to expose the details of your private life to your boss in real time. If using social media is important in your work team, set up a work account.
- Don't identify your employer on your personal social media account. This is another strategy to avoid blurring the line between your personal life and your work, and it gives you some protection against potential claims you are exploiting your employer for your own gain.
- You can blow the whistle on unethical behavior, but not using social media. Public criticism of your employer is risky business; you have a duty of loyalty under the law. If you have a concern about something that's going on at work, talk to a union rep about how best to resolve it. If you're bothered about the way your employer is handling something, don't vent online.
- Don't release information about your employer that isn't already public. If it's not your job to make public announcements, don't make them. You can get into trouble for revealing proprietary information.
- Your work computer is your employer's property. Don't assume that what you do on that computer (or mobile device, if it's supplied by the employer) is private, even if you're using a non-work account. It's company equipment and the company can monitor your computer use.

G. IN THE EVENT THAT YOUR LOCAL IS IN BARGAINING, HERE ARE MORE POINTS TO CONSIDER:

- You can make comments on social media that describe what the company is doing in bargaining and that are critical of the company's position, but be careful to use common sense and good judgment.
- Ensure that what you say in a posting is true.
- A factual public statement or an opinion about collective bargaining or a collective bargaining issue will, in most circumstances, be easier to defend (unless the union and the employer have agreed to keep the subject matter confidential).
- A factual public statement or an opinion that harms the employer's reputation and is about something that is happening in the workplace that is not being addressed in collective bargaining will be more likely to attract discipline and will be harder to defend. Bring those kinds of issues to the union for the union to deal with.

- If you identify yourself as a company employee or are identifiable as such, be clear that the opinions expressed are your own and do not represent the opinion of the employer.

If you are a union official, you have a bit more latitude. Labour legislation gives employees acting in their capacity as union officials a broad, but not unlimited, right to make public statements to promote the interests of their members.

H. SOCIAL MEDIA USE AND THE WORKPLACE IN CANADA

Social media use has become a daily activity for a large portion of the population. Facebook, Twitter, Instagram, Reddit and other forums are commonly used for personal and business purposes. Social media is a powerful communication and networking tool; however, improper use can cause serious damage to a company's reputation, and have a negative impact on employee morale. Despite this many employers do not have effective social media policies in place regarding the use of social media by employees.

Employee conduct on social media has been the subject of both news stories and litigation across Canada. No company wants its reputation to be negatively impacted by a tweet or photo posted by an employee that goes viral. In order to outline the parameters of what is expected of employees, an effective social media policy needs to be integrated into a company's existing policies regarding protection of privacy and confidential information, workplace safety, conduct in the workplace, and discipline. The policy should be reviewed by new and existing employees and training should be provided to ensure that everyone understands what is expected. Given the ever-evolving nature of social media, it is also important for employers to periodically review and update the policy as needed.

I. ENFORCEMENT

With a policy in place, enforcement becomes the next issue. What is an employer to do once it becomes aware that its employee has breached its social media policy? The potential discipline for the employee will depend on the nature of the employee's conduct. At the same time, if the employer has a clear, written social media policy that has been violated by the employee, dismissal may be justified:

Factors:

- Damage to the company; including, reputational damage;
- Damage to the operation of the workplace;
- The frequency, timing and duration of inappropriate posts;
- Response of the employee; e.g. uncooperativeness or defiance when confronted, or honesty and remorse;
- Disclosure of confidential information; and
- Whether previous warnings have been given.