hiring.monster.ca

Why Every Company Needs a Workplace Social Media Policy

7-9 minutes

By: Karin Eldor
Monster Contributing Writer

Social media is a double-edged sword for employers. On one hand it serves as a free promotional tool for your company thanks that allows employees to share work-related photos and positive news on their personal social media channels. On the other hand, it has introduced the need to regulate these communications without stifling them. As Voltaire first said, “with great power comes great responsibility.”

With tech-savvy Millennials in the workforce and now Generation Z

(those born in 1995 or later) on their heels, the lines between "personal" and "professional" have become increasingly blurred online. As a result, your company would do well to maintain certain guardrails to ensure that no trade secrets or brand negativity are publicly shared.

This is why many companies have instituted a workplace social media policy as part of their onboarding or human resources training efforts. This document gives employees a clear understanding of what they are allowed to post on their own channels and what is off-limits.

Without such a policy, your company is at risk of facing legal issues or even a public relations nightmare due to an account hack.

Does your company have a workplace social media policy? Before you start writing one, consider a few basic guidelines.

The Pros Of A Social Media Policy

Remember that two separate social media policies may be necessary:

1. One for each employee's **personal** social media channels.
2. One that relates to the **corporate** social media accounts, which might be managed by several employees. (Community management is usually part of the following departments: Customer Service, Human Resources and/or Marketing / Social Media).

The latter depends on the nature of the business, of course, and doesn't apply to every company.

One important disclaimer for all companies: Whatever you post on social media is written in permanent ink and cannot be permanently erased (even if it can be deleted). And that applies to everyone.

In the event that someone tweets a regrettable statement and deletes it a few minutes later, there's always the risk that someone took a "screenshot" of that post and began circulating it online. That means even deleted posts can go viral. (And you can certainly think of some people in the spotlight or even corporations whose tweets have made headlines. This is the stuff of corporate nightmares!)

By clearly outlining the "dos" and "don'ts" of social media to all employees (as well as store associates, if applicable), you are ensuring that they think twice about sharing a picture or a statement. And this itself is critical, especially considering that for younger generations in the working world, sharing on social media is second nature.

What goes into a social media policy?

The following are some guidelines to consider including in a general social media policy, for all employees. This document should be distributed to everyone as part of their onboarding or training; it can also be rolled out as a new policy for all current employees:

Proprietary information is off-limits: This includes (but is not limited to) photos of upcoming product releases, or any information regarding prototypes, brainstorm sessions and development meetings, for example. This also prohibits retail associates from posting photos of customer receipts (even if the client is a celebrity or purchased a huge order), or the cash register POS system if the store had a record-breaking sales day, for example.

Head office photos can also be questionable: Some companies are secretive about their head offices, and shy away from sharing photos of their headquarters. If this is the case for your company,

be very clear about which rooms are allowed to be featured on social media and which ones are off-limits.

Personal posts on personal social media feeds: When it comes to employees' personal channels, not all areas are crystal clear. Legally, employees are free to post whatever they choose on their personal social media channels (as long as they're not breaking any of that channel's terms and conditions).

And while some employees add a legal disclaimer like ""The opinions expressed on this site are my own and do not necessarily represent the views of my employer" to their Twitter bio, these disclaimers won't be enough to protect an employee who goes on a vulgar rant about their boss or drags their employer's name in the mud after being passed for a promotion.

At the end of the day, employees need to be reminded that whatever they post on social media represents their own professional brand. Therefore, it's important to tread carefully.

Workplace conflicts should stay offline: As tempting as it can be, avoid venting about workplace frustrations or conflicts, whether they involve managers, colleagues or customers. Even harmless posts like: "TGIF: this was a horrible week at work!" can open the door for negative chatter surrounding your company.

Privacy on Facebook, LinkedIn, Twitter, and Instagram: Since LinkedIn and Twitter are open to the public, employees should be even more mindful of what they post on these social networks. If an employee might not want their social activities exposed, then they are best off keeping their Facebook and Instagram feeds set to "private."

Your monitoring of posts: All of this doesn't mean you should go

on a witch hunt to look for employees breaking your social media code of conduct. Simply monitor any brand mentions on social media, with the help of a social media listening tool or doing simple brand name searches on Twitter and Instagram. There can also be a general “if you see something, say something” rule in the case of a disgruntled employee posting threatening language to their social media accounts.

Corporate social media policies for corporate accounts: If some internal employees have access to your corporate social media accounts, then the following two security measures are usually included (and added to the above rules):

File under “data governance or security”: Make sure only a few internal team members have passwords to your company’s social media platforms and update the passwords frequently to minimize any risk of their getting into the wrong hands.

Dealing with ex-employees: If an employee is let go or resigns, make sure you delete that person’s access to all corporate social media channels and change all social media passwords ASAP, to ensure the former employee can't hack the account.

A general guideline for social media policies: All employees are ambassadors of your employer brand. If they are about to post something that they would be ashamed to say out loud, or that can haunt them in the (near term or long term) future, then they should think twice about posting it.

As an employer, you can mitigate this risk by educating employees and protecting your brand at the same time. In an era of oversharing in which everything seems to be fair game, your company will avoid damaging its reputation by having these policies

in place.

Legal Disclaimer: None of the information provided herein constitutes legal advice on behalf of Monster.