

Who Owns Your Company-Sponsored Social Media Account?

09.14.12 01.07.26

Remember when Facebook was just for college kids? Well, things have changed. These days it seems like even giant companies are using social media to show their warm and fuzzy sides and to connect with customers. Obviously, the CEOs of these companies are not spending their time maintaining the accounts and posting clever comments. On the contrary, companies usually dedicate one or more employees to speak on behalf of the company, through a company-sponsored Facebook, Twitter, or other social media account. If done right, an account can build up thousands of followers and grow to host useful information, photos, or communications, becoming an important resource for customers.

But what happens if the employee who is running a company-sponsored account quits? In a perfect world, that employee would gladly relinquish control of the account back to the company. But what if the employee leaves on bad terms? What if the employee leaves for a rival company? What if the employee changes the password and starts posting negative comments, confidential information, or trade secrets? Sorry to get all lawyer-y, but these are the questions that keep me up nights.

To avoid potential negative consequences, employers need to ensure they have maintained control over any and all company social media accounts. This may mean creating strict guidelines for postings on these accounts to ensure the proper message and content are being communicated. (Some of you may be wondering whether this could be at odds with the recent guidance from the NLRB. Have no fear, the NLRB can't get you in trouble for controlling what an employee says when speaking *on behalf of the company*.)

Employers should also make it very clear that, regardless of how much freedom an employee has in maintaining the account, the company is the owner of the account and has the exclusive right to revoke access at any time for any reason. Under your policy, the company should also be the keeper of the passwords and should change them when employees leave. To protect your intellectual property, you should also consider warning employees that all content posted on or created for the social media account belongs to the employer, not the employee who posted it.

It is very easy to update your social media policy to include restrictions like these. Here are a couple of ideas:

- [Company] reserves the right to all relevant, business-related passwords and account information and has the unilateral right to change passwords and block access to a [Company] social media account for any reason. Employees who leave [Company] are required to relinquish any rights to access [Company]

social media accounts.

- Any authorized social media account is the sole property of [Company], and any photographs taken or content created using [Company] equipment or for an official authorized [Company] social media account is exclusively the property of [Company].

The specificity of the restrictions you place on employees will depend on your expectations for employee use of company-sponsored accounts and on your company's culture. Too many restrictions could come across a bit overbearing and send the message that you don't want your employees' help in utilizing social media to promote your business. This would be bad, as social media can be an extremely effective tool in promoting your brand. Too few could get you in a difficult situation if an employee goes rogue. What is clear, however, is that companies that want to use social media to market or otherwise communicate with customers should have protections in place in case things go sour with the employee with the password. For more information, please contact [Greg Duff](#).

Posted in [Employment Law](#)

Tagged as [employees](#), [Facebook](#), [handbook](#), [NLRB](#), [Social Media](#), [Twitter](#)