SMALL BUSINESS ADVOCATE

> What to do (and not do) with your social media policy

by Joseph J. (J.J.) Minioza

Joseph J. (J.J.) Minioza

Social media policies are more important every day because social media is so prevalent in our society and the workplace. Even when websites are blocked on the job, employees using smart phones and social media after hours can directly affect employers. A clear social media policy in your employee handbook is your first line of defense, but what is an employee's expectation of privacy with social media?

Why employers need a social media policy

Recently, media stories have covered employees losing their jobs because they posted inappropriate content on Facebook, Twitter or personal blogs. In most cases, the employee had no idea the content they were posting could be actionable by their employer because they never received a clear social media policy.

Not having a social media policy can expose employers to possible risks:

• Employees identifying their employer while posting inappropriate material about the company, management, co-workers, clients, vendors or others;

• Employers demanding access to employees' social media accounts or asking for usernames and passwords to accounts in interviews;

• Losing or disclosing an employer's confidential information and/or trade secrets;

• Civil liability relating to an employee's inappropriate posting either at or outside of work;

• Reputation threats relating to inappropriate material that has been posted; and/or

• Defamation and discrimination claims by an employee against an employer.

Don't do this

• Screen applicants using social media and/or ask for their passwords to such sites. This may be barred by state and federal law. Screening using social media poses risk for protected class discrimination claims depending on what's posted;

• Adopt overbroad social media policies which may unreasonably prevent protected concerted activities outlined by the National Labor Relations Act (NLRA); and

• Use overbroad third-party apps when accessing applicant and employee information.

What to do

• Create a current, effective and enforceable social media policy;

• Instruct employees not to use vulgar, obscene, threatening, intimidating or harassing language; attack people based on protected status (e.g., union status or activity, disability, national origin, etc.); disparage company products and services; or disclose confidential or proprietary company information;

• Create a companion privacy policy establishing guidelines to safeguard confidential employee or company information. Confidential employee information may include home addresses, birthdays, medical data and protected status information. Proprietary company information could be financial, trade secrets or other business information;

• Use a non-decision-maker to assess applicants if using social media as part of candidate screening;

• Consult with counsel prior to firing or disciplining employees who post questionable social media content to ensure you have cause;

• Check with legal counsel before refusing to hire applicants (or fire or discipline employees) based on information culled from social media;

• Train employees about social media policies; and

• Monitor ongoing legal developments established and implemented by federal and state legislatures, agencies and courts and amend your policy accordingly.

Social media policies must comply with Section 7 of the NLRA, which applies to both union and non-unionized workforces. It states: "Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." An employer that disciplines an employee who engages in "concerted activity" or develops a broad social media policy prohibiting such protected activity violates the NLRA and may also violate 29 USC §158(a)1.

The National Labor Relations Board (NLRB) determined that Facebook, Twitter and personal blogs are platforms where employees may engage in "concerted activity." In August 2011, the NLRB released a General Counsel Report analyzing approximately 14 cases involving social media and alleged violations of the NLRA. (See https://www.nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases). The report does not define what constitutes protected activity, but does cite guidelines for when an employee's use of social media may be considered protected activity.

California's right to privacy law is well-settled but still evolving as social media expands. On Aug. 21, 2012, the California State Senate approved a bill preventing employers from requiring workers to provide passwords to their social media accounts. The bill, AB 1844, passed the senate 37-0.

For more information, call (510) 832-7770. ■

Joseph J. (J.J.) Minioza is an attorney at the Oakland law firm Ericksen Arbuthnot.

Even when websites are blocked on the job, employees using smart phones and social media after hours can directly affect employers.

Source: Oakland Business Review October 2012