Social Media Use Policies – Fact Versus Fiction

With the New Year now upon us, many of you may be reviewing your social media use policies in the coming weeks, in order to determine whether any changes need to be made in either their content or application.

The world of social media is fast-paced and ever-changing. This makes it extremely hard for case law relating to an employer's ability to restrict employee use of social media to keep up with current technology and social trends. Some employers thus are waiting to create a social media use policy until the law is more settled. However, taking this approach will effectively mean a never-ending wait, and can leave you unprotected when an employee's use of social media interferes with their or others' work and/or their (or your!) professional reputation.

On the other side of the spectrum, some employers have enacted broad social media use policies in an effort to be proactive, protect the company's name and reputation, and keep their employees efficient at work. While a solid social media use policy is a "must have" for all employers in this day and age, recent activity by the National Labor Relations Board's (NLRB) General Counsel indicates that an overly broad policy may be just as dangerous to an employer as having no policy at all.

Because updating or creating new policies can be a daunting task, especially amid the other first-of-the-year items on your plate, here is a quick checklist of some things to keep in mind when reviewing or creating your social media use policy.

1. Protect confidential and proprietary information of the company and its clients. Identify the types of information you need to protect and outline in your policy your methods for protecting it. Issuing passwords required to access certain data, restricting their use and disciplining both negligent and intentional abuse of the same thus are key features of a social media use policy. This is especially true for employers in the health care field, as information an employee is sharing on the Internet may not simply be confidential information of your company, but may involve protected health information of a patient, making its dissemination a violation of HIPAA.

2. Have separate provisions for on- and off-duty social media use. While it is of course permissible to restrict an employee's use of company property or time for social media activities, the same broad restrictions are not appropriate regarding an employee's off-duty conduct. Off-duty social media use restrictions must be limited to more content-based restrictions which address issues such as improper dissemination of confidential or proprietary information, harming the image of the employer and/or its products or services, and guarding against incidental product endorsements and testimonials through employee on-line activity which may violate Federal Trade Commission guidelines. Employers also may prohibit off-duty social media use which violates their company policies against harassment or violence in the workplace or which otherwise undermines or interferes with the employee or others' work for the company.

In considering this checklist item 2., however, be mindful of a recent complaint issued by the NLRB's General Counsel which alleges that employer policies which prohibit employees from making "any" disparaging remarks about the employer or its supervisors or which

prohibit employees from depicting the company "in any way" over the Internet without company permission interferes with employee rights under the National Labor Relations Act (NLRA). The full impact of this complaint on employers is not yet known, as the NLRB's decision regarding this complaint has not yet been issued. However, at the very least, this complaint serves to highlight the NLRB's focus on social media use policies – and the fact that it is not going to be shy about challenging employer policies it feels are too broad in light of employee rights under the NLRA. Specifically, the NLRB views overly broad social media use policies as a form of interference with employee rights to engage in protected concerted activity under the NLRA.

Note also that the NLRA protects both union and non-union employees against potential union-related activity and other group action that qualifies as "protected concerted activity." So, non-union employers cannot ignore this new NLRB focus.

The NLRB also is concerned with the effect of the employer's policy, not the employer's intent in drafting it. So, the fact that you may not have "intended" to interfere with your employees' ability to communicate about their work conditions and terms of employment will not matter to the NLRB if your social media use policy is deemed to have this "effect" due to being overly broad in its content-based restrictions.

3. Be aware of employee privacy rights regarding your access and monitoring of employee social media use. Some employers inadvertently create an "expectation of privacy" by providing in their social media use policies or in practice that employees can create "personal" or "private" e-mail files or can use Internet access sites which are password-protected and to which other employees cannot obtain access without knowing the individual employee's chosen password. If you allow such practices, your social media use policy should be clear that a "personal" or "private" or "password-protected" e-mail, Internet or other computer file is still subject to access and monitoring by the company because such files are being maintained on or using company property.

4. Note also that some states have privacy protections beyond federal protections which may apply to social media. It is important to know the protections that apply to your company and the impact of these protections on your social media use policy as far as how much monitoring you can do of your employees' social media activities in the particular state(s) in which you do business.

5. The final way an expectation of privacy can be inadvertently created by an employer, despite saying in its social media use policy that "all e-mails or other communications sent or received using company e-mail systems or other company property are subject to monitoring and access by the company at any and all times" is to never actually monitor or access any employee e-mail or other communications. An employer merely "retaining the right" to do so, but never actually using this right, can become the equivalent in the eyes of the law of waiving this right, such that employees can be deemed to have an expectation of privacy where none was intended by the employer.

These are just a few of the issues to consider as you update your current social media use policy or decide to draft one for the first time this year. Each employment context may present its own specific policy needs and considerations, and will require a well-drafted policy which is tailored to meet these needs.

For more information on this topic, or for assistance in drafting or revising your social media use policy, please contact Sara Anne Thomas at sthomas@millermartin.com or your Miller & Martin Labor and Employment law attorney.

THIS IS AN ADVERTISEMENT.

FOLLOW US ON twitter

Atlanta | Chattanooga | Nashville
www.millermartin.com

ATLANTA

1170 Peachtree Street, N.E., Suite 800
Atlanta, GA 30309-7706

CHATTANOOGA

832 Georgia Avenue, Suite 1000,
Volunteer Building
Chattanooga, TN 37402-2289

NASHVILLE

150 Fourth Avenue North, Suite 1200, One Nashville Place
Nashville, TN 37219