Everyone is on social media these days, including your employees. If employee social media use goes unmanaged, it can cause serious problems for your company. Applying these do's and don'ts will help you manage social media use in an effective, responsible, and compliant manner.

1. Do: Have a Plan to Manage Employee Social Media Use
Employers must have a plan on how to manage social media use in the workplace. Failing to do so can have serious consequences. Employers can be held vicariously liable for legal and regulatory liability arising out of their employees' social media use, such as for an employee's defamatory, discriminatory, or harassing social media message, comment, or tweet. Companies are also exposed to employee leaks of sensitive company or customer information, or for the improper use of the employer's intellectual property and trade secrets. These risks exist regardless of whether the employee commits the offense at the office using company-owned computer resources or at home using their personal social media accounts, since they are often identified as an employee of the company in their social media profile. So having a plan to manage employee social media use is essential.

2. Don't: Simply Fire or Discipline an Employee for their Social Media Posts without Ensuring the Basis is Sound
Many employers do not realize that certain employee social media activity is protected against employer retaliation in the United States. Generally speaking, Section 7 of the National Labor Relations Act protects two or more employees who act together online to improve their terms and conditions of employment. Employees have a protected right to seek help from third parties on social media regarding their working conditions, including conversations with fellow employees and the press. An employer violates Section 8(a)(1) of the NLRA if it interferes, restrains, or coerces employees in the exercise of their rights guaranteed in Section 7. An employer may unlawfully interfere with its employees' Section 7 rights by disciplining or terminating an employee for engaging in protected activities, threatening to sue employees for engaging in protected activities, or discharging an employee to prevent future employee discussions of terms and conditions of their employment.

3. Do: Implement a Social Media Policy
Developing a social media policy makes business and legal sense. A social media policy assists companies in managing employee social media in order to limit exposure to costly legal problems. A social media policy also serves as a communications guideline that empowers employees with the information they need in order to use social media in a responsible manner. Social media policies should contain a mix of social media objectives, values, guidelines, and best practices; rules on what is considered appropriate and inappropriate use of social media; and the governance procedures that the company follows when the rules are broken. Social media policies accomplish these goals by providing formal work rules for social media use by employees. Effective rules include provisions addressing both professional and personal use, and also set forth provisions regarding appropriate language and content. Implementing these work rules can help avoid serious public relations issues that can arise when an employee's inappropriate social media activity goes viral.

4. Don't: Overreach with Your Social Media Policy to Prohibit Protected Activities

Generally speaking, a rule contained within a social media policy violates the NLRA when it precludes employees from engaging in protected concerted activities. This can occur, for example, by setting forth rules that tend to discourage employees from discussing terms and conditions of employment or sharing information about themselves or their fellow employees with outside parties. When an employer's work rules contained within its social media policy are found to have violated the NLRA, the National Labor Relations Board (NLRB) commonly orders the employer to cease and desist the unfair labor practice, rescind or modify the unlawful policy, and post a notice of the violation. Employers commonly experience widespread negative publicity when found to have maintained an unlawful policy or work rule. If an employer fails to comply with the cease and desist order, then the NLRB has the authority to have the employer found in contempt of court, and to have civil and/or criminal penalties imposed on the employer.

5. Do: Ensure the Policy Has Been Reviewed Recently to Ensure NLRA Compliance

Many employers believe that once a social media policy is in place, they have successfully managed social media use in a manner that complies with the NLRA. This would be a mistake. Over the past two years, employer disciplinary actions for employee social media use and employer social media policies have come under the scrutiny of the NLRB. This has resulted in the NLRB issuing three memoranda on social media employment cases that address case developments arising from social media use in the workplace, emerging issues concerning the protected and/or concerted nature of employees' Facebook and Twitter postings, and the lawfulness of employers' social media policies, rules, and disciplinary actions as a result of employee social media activity. Companies that fail to regularly administer a "check up" of their social media policy to ensure the work rules contained therein comply with the NLRB's on-going interpretations of the NLRA in the context of social media often find themselves on the receiving end of a cease and desist letter.

6. Don't: Forget to Implement the Policy on a Company-Wide Basis

After a company is satisfied that it has drafted or revised its social media policy in a compliant manner, it must introduce the policy and any subsequent revisions on a company-wide basis. The policy should be distributed to the company's summer interns, upper-level executives, and everyone in between. Employers should also consider whether to distribute the policies to any independent contractors or other persons who may act on behalf of the company. The policy can be distributed at a company-wide meeting, sent by email, posted on the company web site or intranet, and/or included in the employee handbook. The policy should be read and distributed each and every time a company amends, revises, or makes additions to the policy. Also, the company should retain records of each time the policy was distributed, received, and acknowledged by each person who received it.

7. Do: Train Employees on the Policy and Maintain Comprehensive Records

Employers should educate and train employees about the restrictions within the policy through a formal training program. A formal training program will leave little doubt as to what social media activity is prohibited and the consequences for violating the policy. Providing a formal training program will also demonstrate to investigators, regulators, and to a tribunal that the company is committed to managing social media in a compliant manner. Employers should maintain and manage comprehensive records related to their company's social media policy and training programs, including electronic or hardcopy confirmation that each employee received and reviewed the policy and attended company training. This can be accomplished by maintaining training sign-in sheets or attendance records, signed policy acknowledgment forms, or electronic "read" receipts that confirm that the employee has read the policy, understood it, and agreed to adhere to it.
8. Don't: Fail to Designate a Contact Person
Employers should consider appointing an HR representative, compliance officer, or other employee as the "go to" person for all questions about the social media policy. Designating an employee to handle any questions, comments, and concerns about the policy will ensure that the employer is providing a consistent message concerning the scope and applicability of the social media policy, and will also aid the employer's transparency and facilitate uniform enforcement of the policy. The employer should advise the appointed representative that, to the extent that they are unsure of a response to a specific question by an employee about the policy, they should first consult with in-house counsel prior to providing an "off-the-cuff" response that may misinterpret the scope of work rules contained within the policy.

9. Do: Monitor Your Employees' Social Media Responsibly
Companies have a right and responsibility to monitor how employees are using social media at all times in some jurisdictions. If companies ignore their employee's social media activity, they may end up facing any number of serious problems both internally (tension, morale problems and complaints within the organization), and externally (lawsuits or regulatory action). Some critics say that this is an exaggeration—that most of what people post on social networks is private and perfectly harmless, and has no bearing on their work. Not so. You may discover that your employees are stealing your time, and you would be within your right to discipline or terminate that employee. Discipline of this nature would not violate Section 7 of the NLRA, and the employee misconduct would not have been discovered had the employer not conducted an investigation. However, companies must be mindful to investigate responsibly. For example, employers who search their employees' LinkedIn profiles with a basic, non-"premium" LinkedIn membership may inadvertently tip off employees who are being investigated as they can see who is viewing at their profiles. If you thus suspect that an employee is "moonlighting", or starting a side business on your "time and dime", opt for a premium membership, or for an alternative method of investigation.

10. Don't: Enforce the Policy Inconsistently
Be consistent in enforcing disciplinary measures. Uniform enforcement of the policy will protect the employer in potential litigation, as it gives employees fewer reasons in support of their claims for retaliatory discipline or discharge. Similar violations of the policy should also result in similar discipline. Consistent enforcement of the policy will dissuade a former employee from alleging that the employer singled out the employee or is otherwise acting in a discriminatory manner. Employers should not analyze an employee's social media activity in a vacuum. Before taking action in response to an employee's social media activity, employers should consider the employee's past actions and interactions with other employees, and the employer should determine the "intent" behind a social media post that, at first glance, could appear to violate the social media policy. By considering past conduct or the context within which a statement was made, a seemingly offensive post may actually be the outgrowth of an employee's prior protected and concerted activity, or an attempt to organize other employees.

Conclusion
By applying these do's and don'ts, companies can take a proactive approach for managing employee social media use instead of deciding how to react each time an employee posts, tweets, or communicates online in a negative or irresponsible manner. Companies will also limit liability for costly legal exposure that generally results in the common "fire first, ask questions later" social media scenario.

The information in this Top Ten should not be construed as legal advice or legal opinion on specific facts and should not be considered representative of the views of its authors, its sponsors, and/or the ACC. This Top Ten is not intended as a definitive statement on the subject addressed. Rather, it is intended to serve as a tool providing practical advice and references for the busy in-house practitioner and other readers.