



RAINEY • KIZER
REVIERE & BELL PLC

Jackson Offices

105 S. Highland Avenue
Jackson, TN 38301
and
209 E. Main Street
Jackson, TN 38301
P 731.423.2414

Memphis Office

Morgan Keegan Tower
50 N. Front Street, Ste. 610
Memphis, TN 38103
P 901.333.8101

Thomas H. Rainey
Jerry D. Kizer, Jr.
Russell E. Reviere
William C. Bell, Jr.
John D. Burleson
Gregory D. Jordan
Laura A. Williams
Robert O. Binkley, Jr.
R. Dale Thomas
Deana C. Seymour
Charles C. Exum
Marty R. Phillips
Dale Conder, Jr.
Timothy G. Wehner
Bradford D. Box
Patrick W. Rogers
Angela C. Youngberg
Michael L. Mansfield
Michelle Greenway Sellers
Keely N. Wilson
Amanda C. Waddell
Geoffrey A. Lindley
V. Latosha Dexter
Craig P. Sanders
Mary Margaret Petrinjak
Jonathan D. Stewart
James V. Thompson
Adam C. Crider
Ashley D. Cleek
Erin Melton Shea
W. Paul Whitt
Todd D. Siroky
Jesse D. Nelson
John O. Alexander, IV
Nathan E. Shelby
Chad A. Naffziger
D. Craig Hodge
Cory A. Brown
Michael Burnett Joiner
Joshua B. Dougan

AREAS OF PRACTICE

Litigation
Professional Malpractice Defense
Tort and Insurance Defense
Employment and Civil Rights
Healthcare
Mediation
Business and Finance
Estate Planning, Wills and Trusts

Visit our Website:
www.raineykizer.com

EMPLOYMENT LAW BRIEF

Spring 2010

How Tweet It Is (Or is it?)

Social networking, social media, whatever you want to call it, has taken the world by storm. MySpace, Facebook, Friendster, LinkedIn and Twitter – just to name a few – have become the preferred methods for networking and in some cases, communication. And because they are such a part of our world, the use of these sites by individuals has become a workplace issue. What used to be private is now public. What used to be secret is now exposed for the world to read and see. In-house employee surveys are no longer the only way to gauge how employees feel about the company. Now all an employer has to do is “Google” its name.

This free and open flow of information poses a new set of issues and concerns for employers. What employee’s post can potentially be viewed by co-workers, competitors, partners and even government and law enforcement agencies. Employers face many dangers from their employee’s use of social media, some of which will be discussed below.

Damage to Brand and Image

Companies work hard to develop their brand and their image. What your employees post online can have a negative impact on that image. Your employment brand is driven by what your employees say about working at your company and is expressed in many ways including how they refer to their job or company in the social networks or by looking for a job with another company.

Impact on Business Relationships

All companies have business relationships or partnering efforts that they wish to continuously foster or maintain. Employee misuse of social media has the potential to negatively impact those relationships. Everyone has heard the story of the vice president of a major public relations firm tweeting a negative comment about the hometown of one of his major clients.

Release of Confidential/Proprietary Information

Most organizations have information they consider to be top-secret. Examples include marketing plans, customer lists, and formulas – items typically covered in a non-disclosure agreement. Inadvertent or purposeful distribution of this information could significantly undercut a business initiative or other strategic plans.

Litigation Liability

Defamation/Invasion of Privacy - If your employees post information that is untrue or should not be revealed publicly an employer may become liable under the theories of defamation and/or invasion of privacy. If the topics appear to be within the scope of the employee’s employment or within the employee’s actual or apparent authority, the risk of liability is even higher.

Liability for release of confidential information – In addition to invasion of privacy claims, health care facilities need to also consider the potential for HIPAA violations. In a recent case an OB/GYN employee posted comments on her MySpace page which referred to the number of abortions a patient had, called a collection of patients the “tramp troop” and mocked a patient who she claimed should never reproduce. Although no specific names were given, enough information was provided that the patients figured out she was talking about them and filed a HIPAA complaint with health and human services.

Harassment/Bullying - While a one-time unwelcome electronic message may just be an aberration, a pattern of them could spell problems. Many employees consider what they do off work to be their own private business. However, if a supervisor posts unwelcome messages to a subordinate during work hours or even after hours, there is potential liability for the employer.

(Continued on Page 2)



(Continued)

Drafting a Social/Electronic Media Policy

If an employer is trying to maintain good employee relations, an outright ban on social networking will probably be counterproductive. Such a decision conveys a lack of trust to employees and creates tension within the workplace. However, a policy should be established that explicitly lays out what is and is not permissible, both on the company's network and outside of it. Such policies put employees on notice of the standards of conduct that apply, eliminates an expectation of privacy and forms the basis for disciplinary action.

- **Company Philosophy**

How does the company feel about social networking? Many companies have embraced it and actually use it as a marketing tool. Others are totally against it and do not understand the benefits of it. Your social networking policy should clearly establish the company's philosophy so that there is no misunderstanding by employees.

- **Social Media Use and Work Productivity**

Many employers today do not want to impose an outright ban on all personal use of company resources such as computers and cell phones. In today's busy world, work is sometimes the only time employees may have to check their bank account balances, make a doctor's appointment or reserve a hotel room. When you allow an employee to use resources for these personal activities, it seems harsh to disallow use for the occasional Facebook post or Twitter response.

A good policy is merely to state that personal use of company resources should never interfere with working time and that excessive personal social media activity is prohibited. This allows the employee to feel as if they are valued and trusted enough to be allowed the use.

If an employer decides to impose an outright ban against social media in the workplace, the employer should be aware of the difficulties of monitoring and enforcement. Consistency is the key.

- **Definition of Social Networking Sites**

Every company should have its own written definition of social networking sites. A good solid definition is:

"A Social Networking Site is any internet or mobile based user participation tool used for engaging in, sharing and/or discussing user generated information in the form of text, video, audio, photo or multimedia."

This definition will cover sites such as MySpace and Twitter as well as blogs. Flickr and YouTube.

- **No Expectation of Privacy**

Your policy should inform employees that they have no expectation of privacy in their employer provided computers and electronic equipment and that they have no expectation of privacy for items that are publicly posted on social networking sites. The policy should reserve the right of the company to monitor and access electronic communications and employee computer use.

(Continued on Page 3)



(Continued)

- **Prohibited Activities**

Your policy should provide examples of prohibited activities.

- **Harassment/Discrimination:** A social media policy should complement your existing harassment policy. Just as harassment and discrimination are prohibited in the workplace, employees should understand that even private posts made during non-work hours can constitute a violation of your harassment and/or discrimination policy.
- **Confidential Information:** Social media policies must address the issues of keeping proprietary and personal information confidential. Your policy should make it clear that employees are not to reference any clients, customers or partners without express permission.
- **Identification of employer:** You should determine whether you want your employees to identify you as their employer. Unless the employee is engaging in social networking for the specific purpose of promoting the company, you may want to prohibit listing of your company name on social media websites. If you allow identification, guidelines should be given for the use of pictures/logos, trademarks or other intellectual property of the company. Employees should understand that they have responsibility for representing the company in a professional manner. You should also clarify that an employee who comments on company business must include a disclaimer in his profile or bio that his views are his own and not those of the company. Affirm that the company may hold the employee responsible for any negative or damaging portrayals.

- **Terms of Service and Applicable Laws**

Most social networking sites require users to agree to abide by a Terms of Service document. Your policy should hold employees responsible for reading, knowing and complying with this document except in cases where it contradicts company policy. Further, you should reiterate that employees are responsible for ensuring that they comply with all applicable laws regarding copyright and plagiarism.

- **Discipline**

No policy is complete without the affirmation of the right to discipline for violations of the policy. The policy should spell out that violation of the policy can result in disciplinary action, up to and including termination. ■■