# What's Your Status: Managing Social Media in the Workplace


**Presented by: Danialle Riggins, Esq.**

RigginsPisani
Attorneys At Law

421 South Pine Avenue
Ocala, Fl 34471
352-433-2400
DRiggins@RigginsLawFirm.com

# Table of Contents

## Introduction

If your business does not have an account on Twitter or Facebook, you are behind the times. Studies have shown that companies, small and large, are incorporating social media outlets as a part of the workplace communications and to the world. Do not worry if your business is not tweeting just yet. Surveys show that over half of US business still communicate primarily through traditional emails and intranet forms. What most offices need to consider and to address is the fact that the employees that fill those offices most likely do update their statuses between nine to five.

Most participants in the job market have knowledge of what the Internet, MySpace, Facebook, LinkedIn, Twitter, YouTube, IM, etc., are. The majority of office positions require the use of computers. Once you add desktop plus Internet, there is a high probably that it equals some Facebook time for your employee. The question that each employer needs to ask, "Is this good for my business?" It sounds like it should be a no brainer, "No." The answer is not the same for each employer.

Today's employer needs to address with their human resource departments, supervisors, and then employees the appropriate policies to address social media because it is not going anywhere anytime soon. The issues that need to be address is what restriction, limitations, and security parameters will fit the company; how to regulate the new polices; and the means that the policies and amended will be communicate and enforced upon the employees.

Below you will find some information that will help guide you through these suggestions. There is no cookie cutter formula for every business. Each company will have to look at its purpose, goals, and means to create and then fine-tune its social media policy. No matter what, you need one for your employees, management, and the company.

## Why you need a Social Media Policy

Yes, social media is a fad. It too will die down one day. However, while your next door neighbor's grandmother just posted on her wall that she needs you and your secretary to help her build her third barn in Farmville land, you still have a business to supervisor and run. The wide spread phenomenon knows no boundary when it comes to age, race, economic status- nothing. Therefore, your business/office/ company has to be prepared to handle the possible dilemmas and benefits of social media.

The clearer you are, the better your organization will handle the impact of Twitter through the workday. Each organization needs to give its employees notice of where it stands of social media. If the company plans on using social media as a tool to benefit the workplace and existing operating processes, then technological avenues need to be cleared for such action to place. No matter the company and the employees should feel easier once they know what to expect.

## How to create a Social Media Policy

1. The first step that has to be taken by the powers that be is to determine if the social media is a benefit to the company. Therefore, you would need to look at the purpose and culture of your business. Review your business plan or model. When developing a social media look at your short-term and long-term goals and marketing strategies.

If you are in retail, then you may want to have a social media policy that encourages and rewards social media communications. The more your employees tweet about a product, company event, etc., the more exposure and free advertising you will receive. This is even better if your company has its own profile and account. Each employee can link it back to the company and there is instant monitoring.

If the culture of your business is better served by not being spread over the Internet, then your company can take the easy way of just blocking social networking sites at the company firewall. Your policy would also have to address employee posting from home, in the car, at the movies or any place an employee can use a smartphone. Since you have a company reputation to protect, a policy needs to be in place.

If you office decides to have a free-for-all social media or blocked one, a clear and well-develop company attitude and policy needs to be established before you start drafting. Therefore, you will need to do some research on what is out there. Myspace is primarily social. However, you have LinkedIn, which is more career and professional orientated. Facebook is a mixture of both.

2. Define what social media or social networking is for your company. This sounds easy and hard at the same time. Most people know what Facebook is by now. However, there are dozens of socializing websites for your employees to use. Flickr for the embarrassing pictures. Instant messaging chat rooms during video/computer games can viewed by many and saved by all. Blogs are a key area that each employer may need to address. Blogs give an individual an opportunity to express the millions of opinion one has.

3. **Propriety or confidential information must be covered in your company's policy**. Sometimes employees have to be reminded that they have a duty not to harm their employer. This duty exist even when the employee is off the clock. This duty exist without a contract. Great examples are in the American Red Cross, Best Buy's and Dell's social media policies.

4. The next condition that must be included in any company's social media policy addresses an employee engaging in social media on company time and/or company policy. There are several concerns that an employer has to consider such as broadband, viruses, time management, etc. Productivity can be impacted. Social networking can be excellent tools for developing business relationships and locating resources. On the other hand, they can be big time- wasters. Your policy needs to articulate a happy median for this issue. Refer to the Coca-Cola policy as a guide.

5. Rules for management should be included in your policy when it comes to social media communication only on a personal level. Lower and upper management should have some guidance when it comes to friend or not to friend and the content of their posting. Employers need to be aware of situations that could reveal or suggest favoritism, discrimination, the content being given higher weight due to the author's position. Refer to Kaiser's policy.

6. Each policy should articulate the consequences for a violation of the policy. Remember once something hits the Internet it is almost impossible to retrieve it. The policy should spell out that the violation of the policy can result in disciplinary action, up to and including termination. This portion to refer to any other policies and handbooks that address disciplinary action. This is for consistency.

There are easy means to monitor for possible violations. Employers can set Google alerts and twitter searches. In addition, an employer can have employees' identity personal websites, blogs, profiles that they actively use on social websites.

**Privacy Issues**

**How to use Social Media as a tool for prospective employees**

The hiring process is controlled by both federal and state laws. Nevertheless, an employer can use social media websites to get additional information that may not be included on the resume presented to you. Applicants and employees generally have no expectation of privacy with respect to information in the public domain (i.e. on the Internet generally). I recommend the following two websites that will provide additional information- http://www.kgbpeople.com/ and http://pipl.com/ . In addition, employers are bound by certain state and federal anti-discrimination laws – such as those prohibiting discrimination on the basis of race, gender, age, national origin, disability, genetic information, or sexual orientation – regardless of the source of the information. Employers cannot lawfully consider these protected classes when making hiring decisions, regardless of whether the information is obtained from the applicant's résumé, LinkedIn or Facebook profile, or employment references. **Social media should only be used as one of many tools and sources of information available in the hiring process.**

**Employment Lawsuits and Laws Regarding Social Media**

**"contextual integrity"**
*Rubino v. City of New York*, 2012 WL 373101 (N.Y. Sup. February 1, 2012)

Facts of case: A fifth grade student drowned during a field trip to the beach. The next day a fifth grade teacher with a perfect record and employment history posted on Facebook:

> "After today, I am thinking the beach sounds like a wonderful idea for my 5th graders! I HATE THEIR GUTS! They are the devils (sic) spawn!"

She deleted the update the next day. However, the school administrators had seen it. She was terminated for her status. She exhausted the internal appeals of her termination and sued for

wrongful termination. The court held that termination was too severe. However, the court did believe that the posting was repulsive.

> The Court held that: "[E]ven though petitioner should have known that her postings could become public more easily than if she had uttered them during a telephone call or over dinner, given the illusion that Facebook postings reach only Facebook friends and the fleeting nature of social media, her expectation that only her friends, all of whom are adults, would see the postings is not only apparent, but reasonable."

"**Log-in Information**"

There are not many employers who are requesting social media passwords. If there are employers out there who wish to do so, I would tell them there are other laws that arguably already prohibit this practice. Regardless of what state an employer is in, employers should not seek, request or demand for an applicant's or employee's social media or personal email password. Also employers and management should not "shoulder surfing," i.e. asking an applicant or employee to log into a personal social media account while a representative of the employer is standing over their shoulder and viewing the content on the page.

In *Pietrylo et al. v. Hillstone Restaurant Group*, 2009 WL 3128420 (D.N.J., 2009), (unpublished), the court upheld a jury verdict against an employer who asked employees to provide their MySpace log-in information to supervisors. The employer argued that the employees authorized access when they acceded to the supervisors' requests, and therefore that access did not violate the SCA. However, the employees testified that they were, in effect, under duress; they did not want to disclose their passwords but believed if they did not do so they would be "in trouble."

The jury decided that the supposed "authorization" was a sham, and in fact the employer had violated the SCA. The District Court denied a motion for a new trial, stating that the jury was justified in finding a violation of the SCA and analogous state law.

The 9th Circuit reached the same conclusion with regard to a private website set up by a Hawaiian Airlines pilot, on which he posted bulletins critical of his employer, its officers and the union representing the pilots. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

The plaintiff controlled access to his website by creating a list of people who were eligible to access the website, each of whom had to create a password to enter the site. A company vice-president accessed the site using the names of two pilots on the "eligible" list, with their permission.

In a technical decision parsing the language of the statute, the court decided that, because the two "eligible" pilots never had actually accessed the website, they were not "users" of the service.

Therefore, they were not authorized to grant access to the site, and the access in question did not fall within the exception to liability found in 18 U.S.C. §2701(c)(2).

The court also found that a Railway Labor Act claim, in which the plaintiff alleged that the airline had interfered with protected union activity when it accessed his website, could go to a jury.

**States Laws**

A total of 14 states considered legislation in 2012 that would restrict employers from requesting access to social networking usernames and passwords of applicants, students or employees. Such states as California, Ohio, Illinois, Maryland, Massachusetts, Michigan, New York, New Jersey, South Carolina, etc.

**California**
A.B. 1844
**Status**: July 2, 2012. In Senate. Read second time and amended. To third reading.
Prohibits employers from requiring an employee or a prospective employee to disclose a user name or account password to access a personal social media account that is exclusively used by the employee or prospective employee.

**South Carolina**
H.B. 5105
**Status**: March 29, 2012. To House Committee on Judiciary.
Provides that an employer may not ask an employee or prospective employee to provide a password or other related account information in order to gain access to the employee's or prospective employee's profile or account on a social networking website. The refusal of an employee or prospective employee to provide a password, account information, or access to his account or profile on a social networking website to an employer must not be the basis of personnel action including, but not limited to, employment, termination, demotion, or promotions of the employee.

**Federal Law-**

**Password Protection Act of 2012 ( May 19, 2012 in Committee)**
112th Congress, 2011–2012
To prohibit employers from compelling or coercing any person to authorize access to a protected computer, and for other purposes.

**Stored Communications Act**

Employer access to Facebook and other electronic accounts also has been successfully challenged under the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11, which

is Title II of the Electronics Communications Privacy Act. The SCA makes it an offense to intentionally access, without authorization, "a facility through which an electronic service is provided … and thereby obtain[] … access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. §2701 (a)(1). No liability exists, however, for one who accesses such information with the authorization of a user of that service. 18 U.S.C. §2701(c)(2).

## NOTES