

# From E-Mail to Twitter: Managing in an Electronic Workplace

Presented By Eric Swenson

Managing Director, RSJ/Swenson LLC

CalCPA Education Foundation – Employment Practices Conference

November 11, 2009 – Universal City, CA

---

<b>Social Media - Overview</b> .....	2
Facebook.....	2
My Space .....	2
Twitter .....	2
LinkedIn .....	2
Blogs .....	3
The Waste of Productive Work Time .....	4
Examples of Employer Problems with Internet & Social Media .....	5
<b>Employers Best Practices From Hire to Fire</b> .....	6
Recruiting & Interviewing.....	6
Day-To-Day Management Issues.....	7
Best Practices/Techniques to Reduce Employers’ Liability.....	11
What Your Competitors Are Doing .....	12
Do You Have A Policy?.....	12
<i>Can You Do It Vs. Should You Do It</i> .....	20
<b>Email use and abuse</b> .....	23
<b>Sample Social Media Policies</b> .....	27
Casual/Humorous .....	27
IBM Social Media Policy.....	28

## Social Media - Overview

### Facebook

Facebook is social networking website founded by a Harvard University sophomore in 2004, has hit 300 million users according to a blog post by founder Mark Zuckerberg.

Facebook is the second most visited website in the world, according to page-ranking service Alexa. It is easily the world's most popular social networking site, with as many users as the United States has people. –September 16, 2009

Number of Members: 300,000,000<sup>1</sup>

Monthly Visits: 1.19 billion<sup>2</sup>

Average page views per visitor: 14

Average time user spends on Facebook: 28.8 minutes<sup>3</sup>

### My Space

MySpace is a social networking website. It is owned by, Fox Interactive Media, which is in turned owned by News Corporation. MySpace became the most popular social networking site in the United States in June 2006. MySpace was overtaken internationally by main competitor Facebook in April 2008, based on monthly unique visitors.<sup>4</sup>

Number of Members: 200,000,000+<sup>5</sup>

Monthly Visits: 810 million

Average page views per visitor: 18<sup>1</sup>

Average time user spends on site: 18.1 minutes<sup>6</sup>

### Twitter

Twitter is a free social networking and micro-blogging service that enables its users to send and read messages known as *tweets*. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers who are known as *followers*. Senders can restrict delivery to those in their circle of friends or, by default, allow open access. Users can send and receive tweets via the Twitter website, Short Message Service (SMS) or external applications.

Number of Members: 14,000,000<sup>7</sup>

Monthly Visits: 54.2 million

Average page views per visitor: 7.15

Average time user spends on site: 8 minutes

### LinkedIn

LinkedIn is a business-oriented social networking site launched in May 2003 mainly used for professional networking.

The purpose of the site is to allow registered users to maintain a list of contact details of people they know and trust in business. The people in the list are called Connections.

Users can invite anyone (whether a site user or not) to become a connection.

Employers can list jobs and search for potential candidates.

Job seekers can review the profile of hiring managers and discover which of their existing contacts can introduce them.

Number of Members: 45,000,000+<sup>8</sup>

Monthly Visits: 42.7 million

Average page views per visitor: 9.32

Average time user spends on site: 6.5 minutes

### Blogs

A blog (a contraction of the term "weblog") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order. "Blog" can also be used as a verb, meaning to maintain or add content to a blog.

Many blogs provide commentary or news on a particular subject; others function as more personal online diaries. A typical blog combines text, images, and links to other blogs, Web pages, and other media related to its topic. The ability for readers to leave comments in an interactive format is an important part of many blogs. Most blogs are primarily textual.

Number of U.S. Residents who have a blog: 132,852,000<sup>9</sup>

No statistics available on how much time is spent reading blogs.

## The Waste of Productive Work Time

For many American workers today, time's a wastin' - literally. The average worker admits to frittering away 2.09 hours per 8-hour workday, not including lunch and scheduled break-time.<sup>10</sup> As a matter of practice, companies assume a certain amount of wasted time when determining employee pay. However, employees are wasting about *twice* as much time as their employers expect. Employers spend \$759 billion per year on salaries for which real work was expected, but not actually performed.

The biggest distraction for respondents? Personal Internet use. 44.7% of the more than 10,000 people polled cited web surfing as their #1 distraction at work. Socializing with co-workers came in second at 23.4%. Conducting personal business, "spacing out," running errands, and making personal phone calls were the other popular time-wasting activities in the workplace.

<b>Top Time-Wasting Activities</b>	<b>(%)</b>
<b>1</b> Surfing Internet (personal use)	44.7%
<b>2</b> Socializing with co-workers	23.4%
<b>3</b> Conducting personal business	6.8%
<b>4</b> Spacing out	3.9%
<b>5</b> Running errands off-premises	3.1%
<b>6</b> Making personal phone calls	2.3%
<b>7</b> Applying for other jobs	1.3%
<b>8</b> Planning personal events	1.0%
<b>9</b> Arriving late / Leaving early	1.0%
<b>10</b> Other	12.5%

Employees say they're not always to blame for this wasted time, however. 33.2% of respondents cited lack of work as their biggest reason for wasting time. 23.4% said they wasted time at work because they feel as if they are underpaid.

<b>Top Time-Wasting Excuses</b>	<b>(%)</b>
<b>1</b> Don't have enough work to do	33.2%
<b>2</b> Underpaid for amount of work	23.4%
<b>3</b> Co-workers distract me	14.7%
<b>4</b> Not enough after-work time	12.0%
<b>5</b> Other	16.7%

## Examples of Employer Problems with Internet & Social Media

Social networking sites are the root of four problems.<sup>11</sup>

*Loss of productivity:* According to a study by information security consultancy Global Secure Systems and the organizers of the Infosecurity Europe trade show, the use of such sites is costing U.K. business an estimated \$12.5 billion per year in terms of reduced output. Another study showed that employees spend at least 30 minutes a day visiting these sites with some employees spending up to three hours of their working day taking care of their online profile.

*Social engineering and phishing:* This can result in data or identity theft. Most people would not divulge certain details to strangers but it is amazing what data can be gleaned from social networking sites--personal e-mail addresses and even social security numbers!

*Sites are attractive to hackers and spammers:* Social networking sites are attracting hackers armed with malware of all kinds: spyware, viruses and online scams. Hundreds of applications being developed for these sites are used as launch pads of malware such as Trojans.

### The Challenge For Employers

- 17 percent disciplined an employee for violating blog or message board policies. Nearly 9 percent reported terminating an employee for such a violation (both increases from 2008, 11 percent and six percent, respectively).
- 15 percent have disciplined an employee for violating multimedia sharing/posting policies in the past 12 months, while 8 percent reported terminating an employee for such a violation.
- US companies are experiencing an increase in “exposure incidents” involving sites like Facebook and LinkedIn as compared to 2008 (17 percent versus 12 percent). US companies are now taking a much more forceful approach with offending employees – 8 percent reported terminating an employee for such a violation as compared to only four percent in 2008.
- Short message services like SMS texts and Twitter also pose a risk. 13 percent of US companies investigated an exposure event involving mobile or Web-based short message services in the past 12 months.<sup>12</sup>

## Employers Best Practices From Hire to Fire

### Recruiting & Interviewing

More than one in five employers search social networking sites to screen job candidates.

Of the hiring managers who use social networks, one-third said they found information on such sites that caused them to toss the candidate out of consideration for a job, the survey said.

The study found that the number of hiring managers that are turning to social networks like MySpace and Facebook to delve into candidates' online behavior is increasing quickly: Some 22% of employers said they already peruse social networks to screen candidates, while an additional 9% said they are planning to do so. Only 11% of managers used the technology in 2006.

The top areas of concern found on social networking sites include:

- Information about alcohol or drug use (41% of managers said this was a top concern)
- Inappropriate photos or information posted on a candidate's page (40%)
- Poor communication skills (29%)
- Bad-mouthing of former employers or fellow employees (28%)
- Inaccurate qualifications (27%)
- Unprofessional screen names (22%)
- Notes showing links to criminal behavior (21%)
- Confidential information about past employers (19%)

The study did find that 24% of hiring managers found content on social networks that helped convince them to hire a candidate. Hiring managers said that profiles showing a professional image and solid references can boost a candidate's chances for a job.

"Hiring managers are using the Internet to get a more well-rounded view of job candidates in terms of their skills, accomplishments and overall fit within the company," said Rosemary Haefner, vice president of human resources at CareerBuilder.com. "As a result, more job seekers are taking action to make their social networking profiles employer-friendly. Sixteen percent of workers who have social networking pages said they modified the content on their profile to convey a more professional image to potential employers."<sup>13</sup>

- The laws that place limits on online background searches

- A detailed procedure that can be employed in any organization to best protect against future claims
- How to determine what online information is and is not relevant to hiring decisions
- Search methods least likely to generate dangerous information about candidates
- Policy Focus: We'll also use this session to discuss approaches for developing policies that govern your recruiting staff's mining of online information.
- Speaker: Molly DiBianca

### **Is an Internet "Google" search a consumer report?**

What you learn about an applicant from an Internet search engine like Google, MSN, or Yahoo may include information about the person's "character, general reputation, personal characteristics, mode of living," or even credit worthiness. However, to be a "consumer report," the information must be assembled by a "consumer reporting agency" that "regularly" prepares reports for a fee to employers. A search of a person's name through an Internet search engine does not appear to meet this definition.

But, the risk of relying on such a source to screen employees is equal to that of checking any Internet site: You have no assurance that the information you retrieve is about the person you want to check. And even if it is, you have no assurance it is accurate.<sup>14</sup>

### Day-To-Day Management Issues

Blogs, social networking sites, and YouTube™ videos all sound (and look) pretty cool. But before you dive into the social media pool, beware of the deep end that's fraught with lawsuits and other legal trouble. Learn the critical role that HR must play in navigating employees away from these legal dangers during work hours -- and why it's just as crucial to pay attention to employees' social media habits after they're off the clock.

#### *Key Learning Objectives:*

- Examples of "social media experiments" that have taken a turn for worst
- The legal risks associated with employees posting content on a company-run blog or social networking site
- What you should do if you stumble upon the company logo on an employee's personal Facebook page
- Actions that employers can take to protect proprietary information and sensitive employee information
- How to protect your organization from litigation surrounding employee usage of social media tools -- at work and after hours
- The risks of monitoring an employee's personal social media habits and the limits to observe to avoid legal trouble

- **Policy Focus:** We'll show you best-practice examples of company policies that help employees understand the “rules of engagement” associated with workplace social media tools.
- **Speakers:** Molly DiBianca and Jerry Stevenson

Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds<sup>15</sup>  
*Career Expert Provides DOs and DON'Ts for Job Seekers on Social Networking*

**CHICAGO, August 19, 2009** - As social networking grows increasingly pervasive, more employers are utilizing these sites to screen potential employees. Forty-five percent of employers reported in a recent CareerBuilder survey that they use social networking sites to research job candidates, a big jump from 22 percent last year. Another 11 percent plan to start using social networking sites for screening. More than 2,600 hiring managers participated in the survey, which was completed in June 2009.

Of those who conduct online searches/background checks of job candidates, 29 percent use Facebook, 26 percent use LinkedIn and 21 percent use MySpace. One-in-ten (11 percent) search blogs while 7 percent follow candidates on Twitter.

The top industries most likely to screen job candidates via social networking sites or online search engines include those that specialize in technology and sensitive information: Information Technology (63 percent) and Professional & Business Services (53 percent).

### **Why Employers Disregarded Candidates After Screening Online**

Job seekers are cautioned to be mindful of the information they post online and how they communicate directly with employers. Thirty-five percent of employers reported they have found content on social networking sites that caused them not to hire the candidate. The top examples cited include:

- Candidate posted provocative or inappropriate photographs or information - 53 percent
- Candidate posted content about them drinking or using drugs - 44 percent
- Candidate bad-mouthed their previous employer, co-workers or clients - 35 percent
- Candidate showed poor communication skills - 29 percent
- Candidate made discriminatory comments - 26 percent
- Candidate lied about qualifications - 24 percent
- Candidate shared confidential information from previous employer - 20 percent

Fourteen percent of employers have disregarded a candidate because the candidate sent a message using an emoticon such as a smiley face while 16 percent dismissed a candidate for using text language such as GR8 (great) in an e-mail or job application.

"Social networking is a great way to make connections with potential job opportunities and promote your personal brand across the Internet," said Rosemary Haefner, Vice President of Human Resources at CareerBuilder. "Make sure you are using this resource to your advantage by conveying a professional image and underscoring your qualifications."

Haefner recommends the following DOs and DON'Ts to keep a positive image online:

1. DO clean up digital dirt BEFORE you begin your job search. Remove any photos, content and links that can work against you in an employer's eyes.
2. DO consider creating your own professional group on sites like Facebook or BrightFuse.com to establish relationships with thought leaders, recruiters and potential referrals.
3. DO keep gripes offline. Keep the content focused on the positive, whether that relates to professional or personal information. Make sure to highlight specific accomplishments inside and outside of work.
4. DON'T forget others can see your friends, so be selective about who you accept as friends. Monitor comments made by others. Consider using the "block comments" feature or setting your profile to "private" so only designated friends can view it.
5. DON'T mention your job search if you're still employed.

### **Bosses should set social networking rules**

BY BRIDGET CAREY

[Poked@MiamiHerald.com](mailto:Poked@MiamiHerald.com)

Two messages to the working world on social networking sites:

*Dear Employees: Your tweets are making us, and your boss, reach for the Maalox.*

Instant communication is causing headaches, if not ulcers, for many CEOs.

That's especially true when employees hooked on Twitter and Facebook don't think before sharing insider information.

Employees need to realize some conversations are privileged. Just because you're in a meeting about a new product, or worse, layoffs, doesn't mean you should be broadcasting details to the world.

*Dear Bosses: You really should talk to your employees about what shouldn't be shared.*

If there's a meeting going on and you don't want people to talk about it publicly, say so.

Not everyone has the mind-set that everything in staff meetings is private. That's because many employees -- especially millennials like Bridget who spent their college years on Facebook -- don't think about the consequences of sharing work news.

They don't see a reason to not share information, nor that there could be negative consequences to sharing.

Many companies and organizations like the NFL are creating social networking policies that spell these things out. Others have gone to the extreme of simply blocking social networking.

Last week, the Miami Dolphins said they were clamping down on players and media tweeting during practice.

Companies shouldn't think of social networking sites as inherently good or bad -- they're just the most recent form of communication. So why not communicate with your workers about what's appropriate and what isn't?

It is a two-way street. Workers should think about whether it makes sense to be talking about things that are public knowledge but sensitive, like layoffs or strategy.

Do you really want your boss to see you broadcasting not-so-great news about your company? How much of an asset are you if you're reminding the world of bad news?

And more importantly, why would someone want a complainer on their team?

### **Sexual harassment is much more subtle, and harder to confront<sup>16</sup>**

Much of the problem is that newer technology — e-mail, IM, texting or posting on social-networking sites — makes it much easier for comments to be misconstrued on many levels.

When you talk in person, 80 percent of what you say is in your tone and body language. With technology, all of that is gone. If you admire an employee's new haircut while she is in your office, she can read your tone and body language; and you can read hers. However, a late-night text message admiring your employee's new haircut can take on a lascivious tone, even if that is not the intention.

A 27-year-old professional woman tells the story of how one of her superiors, a flirty married man with children, who, after overhearing a previous comment she'd made to a

female co-worker about buying a new dress, sent her a late- night e-mail from his personal account, telling her he couldn't wait to see her in the dress.

"I'm sure you will look amazing in it," he wrote. The woman responded that she didn't appreciate him sending an e-mail like that to her work account, and he claimed it was a mistake and "half-apologized." Later, he sent her an IM that she feels was "completely inappropriate." She remembers telling her co-workers she would have to block him.

The woman says she never reported the incidents to her direct superior or human resources. "With a staff that small, I knew that any complaint would be public knowledge within seconds," she says, "and I didn't have someone I could go to and feel safe talking about a sexual harassment policy."

Sometimes employees don't understand that if you are at home, and send something from a private e-mail account to a co-worker, that it can still be used against you."

And because electronic conversation is such an integral part of office communication, people might feel compelled to respond to it, even if the message makes them uncomfortable. "Someone might write back 'LOL' just to say something, and then the person thinks what they wrote is welcomed," says Bowman, who adds that emoticons can also be a source of misunderstanding: "People use those little winks. Those things can be completely misconstrued, on both ends."

Social-networking sites like Facebook and MySpace can be another potential source of trouble. "Sites like this can become fertile ground for someone's fantasy life," says Brenner. "If you're trying to maintain a professional stance at work and don't want any entanglements, be careful about what you put up." Innocent vacation photos of you in your bikini may unwittingly draw unwanted attention at work. Brenner recommends having separate profiles for professional and personal contacts, or just sticking to a professional site like LinkedIn for your work colleagues.

### Examples of Employee Issues in the Workplace

#### Best Practices/Techniques to Reduce Employers' Liability

##### **What can businesses do?**

There are three options.

1. Ban access to social networking sites (in an extreme case--block all Internet connectivity).
2. Allow employees unrestricted access, confident that they will only use it during their lunch break and they will not download material on to the network.

3. Monitor and limit staff access to these types of sites, including general Internet browsing and downloading.

Banning internet access outright is obviously counterproductive while allowing uncontrolled Web browsing is tantamount to leaving the front door to one's house open with the key in the lock.

The middle ground monitors all Web activity and controls it on a per user basis when social networking sites can be accessed at the office. Administrators can use Web monitoring software to block access during most of the day except during the staff lunch break or before and after normal office hours. The same software can be used to ensure that any files downloaded or links accessed online are checked in real time for exploits, malware and viruses.

If a company wants to make use of a social networking profile for marketing purposes, access should be given to those who will be updating the profile and all content should be monitored to ensure it is appropriate. Running third party applications should be discouraged.

Education also is important. If an organization wants its employees to be given restricted access to their social networking profile, it must be made clear to them that they need to be vigilant, avoid clicking on links that are suspicious, refrain from downloading files or applications that may be infected, and limit what details they add to their profile--details that could be used to steal identities and commit fraud.

Hackers are attracted to social networking sites because they see the potential to commit fraud and launch spam and malware attacks. Organizations, on the other hand, need to be made aware of the security risks involved and take the steps necessary to safeguard their systems and data yet allow the company to make the most of what the Internet and social networking have to offer.

*David Kelleher is communications and research analyst at GFI.*

### What Your Competitors Are Doing

#### Do You Have A Policy?

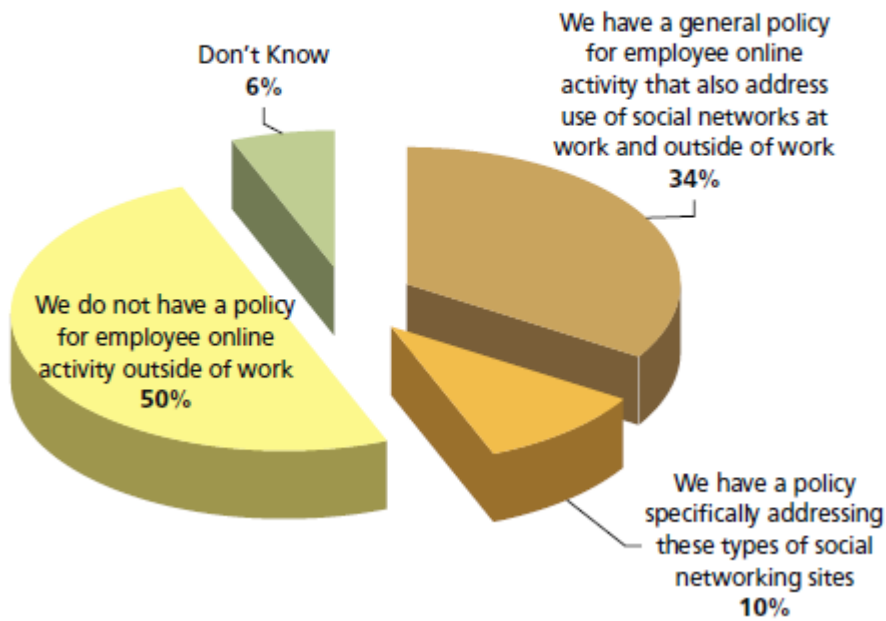
More than 50 percent of companies questioned said they have no policy to address the use of social networking by employees outside the workplace.<sup>17</sup>

Typically, companies shy away from restricting an employee's actions off the job. But businesses are concerned about employees who use social networking and reveal private details or post inappropriate pictures that could embarrass the company.

Some organizations, such as the U.S. Marines, have already banned their recruits from using Facebook and Twitter. But the survey found that many businesses aren't sure what to do to restrict or monitor such usage.

Of the companies questioned in the survey, 34 percent said they have a general employee policy that addresses all online activity, including the use of social networking, both on and off the job. Only 10 percent said they have a policy specifically geared toward social networks.

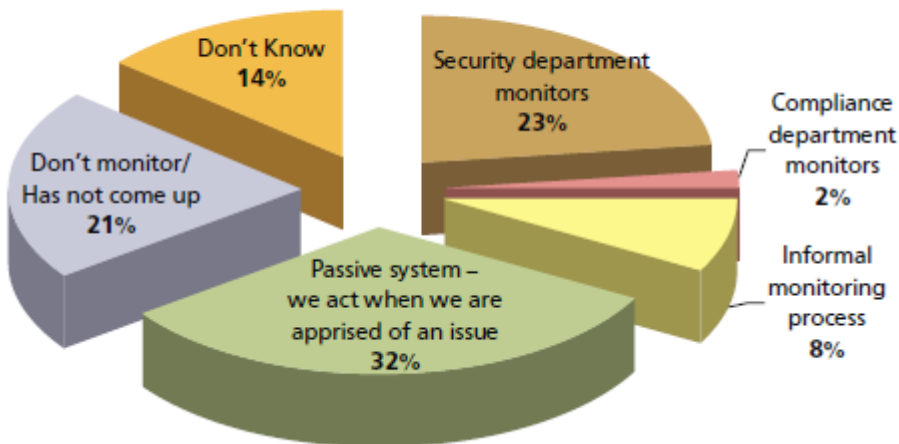
**Does your company have policies specifically addressing employee use of Facebook, Twitter, LinkedIn and other social networking sites?**



()

More than half of the individuals said their company has no active system to monitor employees using social-networking sites. Around 32 percent said their company acts only when an issue is discovered.

**How is employee activity monitored on Facebook, Twitter, LinkedIn and other social network sites?**



Of those surveyed, 24 percent said an employee in their company had been disciplined for inappropriate behavior on a social network, while 37 percent did not know. The percentage was higher in the nonprofit sector, noted the survey, with 33 percent reporting an employee incident versus only 13 percent in the for-profit sector.

"Business clearly hasn't caught up with what its employees are doing online," said Roy Snell, CEO of the Society of Corporate Compliance and Ethics. "The risks are twofold. First there remains the business risk of employees doing things online that may reflect badly on the company. The second is that, as business develops policies and procedures in this area, there are going to be a lot of people finding that what they have long done is no longer acceptable at work. During the adjustment period there is likely to be a great deal of friction created."

In statistics which hardly surprise, given the number of problems employees have caused for themselves on Facebook and Twitter recently, employees are cracking down on the use of social networks in the workplace.

ScanSafe's latest analysis of over a billion web sites discovered that over three-quarters of companies now block social networking sites — up 20% in the last six months.

As well as the supposed benefit in productivity from blocking non-work sites that can sap employee time (though a blanket ban may be counter-productive and a restricted hours policy might be better for morale) there's also the reduced risk of malware creeping into a company's systems, as well as saved bandwidth.

"Social networking sites can expose businesses to malware and if not used for business purposes can be a drain on productivity and bandwidth," said ScanSafe's director of product management, Spencer Parker. "Given the option, companies are increasingly taking a sterner approach to the sites that their employees are allowed to access. I imagine before long, social networking will be up there with pornography in terms of categories blocked."

It's a fine balancing act. Some companies are using social networks for business purposes, but where is the line drawn?

Does a blanket ban actually sap employee productivity? Might it be better to allow the use of Facebook et al during lunchtime rather than not at all?

<http://www.blogherald.com/2009/08/19/employers-getting-tough-on-social-network-use-at-work/>

Why You Can't Ignore Social Networking Sites  
September 11, 2009

Excerpted from New York Employment Law Letter written by attorneys at the law firm of Epstein Becker & Green, P.C.

Over the last several years, social networking websites like Facebook, MySpace, LinkedIn, and Twitter have evolved to the point where most employees use at least one, if not several, of them throughout each day. Social networking sites provide an easily accessible medium for individuals to stay in contact with friends, colleagues, clients, prospective clients, and the public at large.

People can create their own "personal brand" and connect with hundreds, thousands, and sometimes even millions of people who visit the Internet on a daily basis. With Twitter, for example, a person can offer almost instantaneous commentary on the "news" of the day, whether it's personal, professional, communal, or political, all with a couple of keystrokes and without any filter.

In conjunction with social networking sites, employees (and seemingly everyone else) have taken to blogging to record their thoughts, impressions, observations, and opinions on webpages that can be accessed from virtually anywhere in the world. With the good comes the bad, however, and unfettered employee access to social networking sites, blogs, and the Internet presents a myriad of problems for employers.

Data leakage (or loss) prevention is currently one of the hottest areas in security. Companies are looking for ways to prevent company confidential and proprietary information from slipping through the firewall. Most incidents probably occur via email or file transfers but IM chat tools, blog posts, Twitter messages and even online resume content could disclose proprietary company information. Even using social networking sites on company time or using company resources could be a violation of the company's acceptable use policy. Before you become the corporate poster child for some publically humiliating episode from using social networks at work, check your corporate AUP to make sure you aren't violating the policy.

### **Legal issues and concerns for employers**

Employers need to be diligent to protect their company's interests from disclosure or infringement by employees who use social networking sites or blogs. Blogging in particular poses the greatest potential risk for employers and presents the greatest need for employer control.

A blogger prepares entries and posts them on a webpage precisely so others -- including strangers -- can read them and even comment on or discuss them further. The blogger's posts remain in cyberspace indefinitely, ready to be discovered by wandering eyes after someone has searched the Internet using keywords that locate the blog entry. In a flash, the fleeting complaints of yesteryear transform into a record that may be accessed by a competitor or government regulator or read by a coworker or manager who was

criticized or ridiculed. Or the blog could be viewed by a recently interviewed candidate who is deciding whether to accept a job offer, or by an executive of a company involved in negotiations to buy your company. In the end, you must thoughtfully and prudently respond to what your employees elect to do in cyberspace.

Employers must also seek to protect confidential and proprietary information vital to their business: business plans, new products or services, customer and client information, financial results (particularly for publicly traded companies and those involved in sale or merger negotiations), and trademarks and service marks. The list of confidential and proprietary information varies by industry and employer, but the need to trust employees and ensure they are maintaining those confidences is common to all employers.

Employers also need to protect their, and their employees', reputation from embarrassing or offensive blog posts or the projection of an image they don't want to be associated with (*e.g.*, white supremacy or sexual perversion). Finally, employers still have an interest in maintaining employee morale and discipline despite the proliferation of employees' use of social networking sites and blogging. You must ensure that bloggers and social networkers don't challenge the authority, competence, or personal qualities of managers and coworkers or engage in harassment or disparagement of coworkers.

You can face potential liability from employee use of social networking sites or blogging in a variety of ways:

- **Slander, defamation, and libel.** Your company could be held liable if an employee posts negative statements about another person or a competitor on a website or blog.
- **Trade secrets and intellectual property infringement.** The disclosure of certain trade secrets can destroy the "confidential" status of the information, and the disclosure of a third party's confidential information could lead to an action for trade secret misappropriation or intellectual property infringement.
- **Trade libel.** Misstatements or misrepresentations about a competitor could lead to claims of trade libel.
- **Securities fraud and gun-jumping.** Publicly traded companies can face sanctions for securities fraud if material misrepresentations are posted. Any postings plugging the registered company could violate federal securities law.
- **Employment actions.** Employees may try to sue you for wrongful termination or discrimination if their employment is terminated because of postings that reference personal aspects of their life (*e.g.*, marital status or sexual orientation).
- **Harassment.** Language that is harassing, discriminatory, threatening, or derogatory could prompt a lawsuit.

### **Adapting to the new digital media**

Because social networking sites present new issues for the workplace, it won't be sufficient to rely on an old e-mail policy in most cases. Your approach to drafting a policy that covers social networking will depend on the benefits, risks, and needs of your company. While some businesses will ban access to all social networking sites, others may find that it's advantageous to allow employees access to certain sites or even to create a company webpage on a social networking site.

Companies should tailor their policies to fit their needs. One thing to consider is how to regulate what an employee writes about your company on his profile page or blog. Some companies have instituted policies requiring employees to identify themselves when discussing the company in any public forum (including online forums) to notify readers that they are speaking in an individual capacity, not as a company representative. Other companies, however, may impose strict discipline on employees who post anything about their employer or coworkers.

Set forth your expectations and rules for Internet use (whether it occurs off-duty or at work) through an appropriate policy. Your policy may be part of a broader policy that addresses all media, including e-mail, instant messaging, Internet browsing, and using social networking sites. A clear policy on Internet use should, at the very least:

- Include a specific statement of what is prohibited on employee profiles or logs. You may want to prohibit some or all of the following:
  - disclosing confidential or proprietary information;
  - disclosing the name of the business in personal websites or purely social networking sites except professional networking sites (*e.g.*, LinkedIn);
  - revealing the name of the company on a site with sexual or violent content;
  - using the company's intellectual property (*e.g.*, trademarks);
  - infringing on the intellectual property rights of others;
  - making statements adversely affecting the company's interests or reputation;
  - criticizing customers or other important business partners;
  - making statements supporting competitors;
  - issuing defamatory, harassing, or disparaging language;
  - issuing content that violates the law (*e.g.*, obscenity); and
  - writing or commenting on content that would constitute a violation of any other policies, rules, standards of conduct, or requirements applicable to employees.
- Include a clear statement of what is permitted only with prior approval from the company, such as blogs or postings that imply employer sponsorship or support, use any logos, trademarks, or service marks, or use company time, facilities, supplies, or resources.
- Identify required disclosures, disclaimers, and endorsements, if applicable; and

- Describe inappropriate content, with examples as necessary. Clear direction will certainly help you allow employees to engage in social networking or blogging while retaining the ability to properly monitor and control their computer use.

### **Bottom line**

Whether your company uses social networking sites or not, you need to be aware that your employees are unquestionably using them. Reexamine your electronic communications policies to protect your confidential information, reputation, and trade secrets and ensure that you've addressed social networking sites and blogs. That will help protect you against liability and litigation (from both outside and within your organization) resulting from an employee's Internet postings.<sup>18</sup>

A recent report by Global Secure Systems and Infosecurity Europe UK found that social networking sites like Facebook, MySpace and Bebo cost businesses as much as 6.5 billion pounds (\$12 billion) a year in lost productivity, according to an article in the SiliconRepublic.

The report – which surveyed 776 office workers of their social networking habits – most workers claimed to have spent at least 30 minutes a day on social networks.

More companies are blocking Facebook and Twitter, study finds  
Assume that you're being monitored, expert advises  
By David Wylie, Canwest News Service August 21, 2009

A growing number of employers are refusing to be Facebook's friend.

Companies around the world are increasingly choking off their employees' access to social-networking websites, such as Facebook, Twitter and MySpace, says ScanSafe, one of the Internet's biggest security providers.

In the past six months alone, there's been a 20-per-cent increase in the number of companies blocking such websites, says ScanSafe, which released a study on the phenomenon this week.

"When web filtering first became an option for companies, we generally saw them block access to typical categories, such as pornography, illegal activities and hate and discrimination," said ScanSafe spokesman Spencer Parker.

"I imagine, before long, social networking will be up there with pornography in terms of categories blocked."

The company says 76 per cent of its customers are now choosing to stonewall social-networking sites, a higher percentage than those who block online categories such as shopping, weapons and alcohol.

ScanSafe analyzed more than a billion web searches each month for its study.

Parker said social-networking sites can open the door to viruses, as well as being a drain on productivity and bandwidth.

James Norrie, the associate dean and professor at Ryerson University's Ted Rogers School of Management, harshly criticized the trend.

He said banning employees from using social-networking sites is "one of the most awful things businesses can do to themselves.

"The whole notion of trying to take technology away from [workers] is as good as spanking them and sending them to their room," said Norrie.

Instead, companies should be teaching their employees to use social media so they can promote the company's brand online, he suggested.

Taking the privilege away will only encourage skilled workers to seek out more dynamic employers, he said.

"What employer that wants to be seen as progressive and attractive for a new generation of workers would think that it was good for their employee brand to block access to social computing sites?" Norrie said.

"If they keep putting their heads in the sand, they'll fall so far behind that someone else will be eating their lunch."

David Zweig, who teaches human resources at the University of Toronto, said ScanSafe's global numbers are a good reflection of the current trend here in Canada.

"We don't have very good stats in terms of how much employee monitoring takes place in Canada, but it is certainly on the increase," he said, adding Canadian employers are also increasingly monitoring e-mail.

"Employees must assume that what they're doing at work is being monitored, and act accordingly."

Zweig said when people are spending time on social-networking sites they're not working, so it's easy to see why employers would want to block employees from accessing the sites.

"They want to stop people from potentially wasting time at work surfing these sites, especially if it's not job relevant," he said.

Still, Zweig said employers need to communicate clearly to their employees what sites they're blocking and why or face the prospect of employee deviancy from workers who feel that their employers don't trust them or that they're being treated unfairly.

"They'll do things to get around the electronic gaze, for example," he said. "It can actually create a vicious cycle where doing this actually creates more deviant behaviour to get away from these restrictions and controls."

ScanSafe also found an increase in the number of companies choosing to block websites about travel and sports, as well as web-based e-mail.

© Copyright (c) The Vancouver Sun

### Can You Do It Vs. Should You Do It

#### Five Things to Consider for your Social Media Guidelines for Employees<sup>19</sup>

- How does the use of social media affect employee productivity? Do you want employees accessing social media sites at work for either personal or business relations?
- What legal issues do your company, or vertical, face regarding proper disclosure and/or advice?
- After all, small print exists for a reason, and it's usually not contained within 140 characters.
- What restrictions should employees have when interacting? Like it or not, they will be perceived as a representative.
- How will you train them on the use of these social media guidelines? It's one thing to establish guidelines, but they're failing if employees do not understand, or know, about them.
- What will the repercussions be for violations? Are you willing to enforce them?

According to a recent Deloitte<sup>20</sup> study, this is how others feel:

- 74% of employees surveyed say it's easy to damage a company's reputation on social media.
- 58% of executives agree that reputational risk and social networking should be a board room issue, but only 15% say it actually is.
- 53% of employee respondents said their social networking pages are none of their employers' business.
- 40% of business executive respondents disagree, and 30% admit to informally monitoring social networking sites.

- 61% of employees say that even if employers are monitoring their social networking profiles or activities, they won't change what they're doing online — they know it's not private, and have already made significant adjustments to their online profiles.
- **Would a company policy change how you behave online? 49% of employees say “no.”**



## Email use and abuse

An ePolicy that is well-written and effectively communicated to all employees is one of the best ways for employers to protect themselves from workplace lawsuits and other risks associated with the inappropriate use of corporate software, eMail, and Internet systems.

- **Sexual Harassment**

- Employee misuse of corporate eMail can result in six-figure litigation costs and million-dollar legal settlements. In one high-profile case, Chevron Corp. in 1995 was ordered to pay female employees \$2.2 million to settle a sexual harassment lawsuit stemming from inappropriate eMail circulated by male employees. The offenders' eMail messages included, among other gems, *25 Reasons Why Beer is Better Than Women*.

- **Wasted Talent**

- Xerox fired more than 40 employees for idling away up to eight hours a day on X-rated sites. The downloading of porn videos was so pervasive, it actually choked Xerox's computer network and prevented employees from sending and receiving legitimate eMail.
- Dow Chemical fired 64 workers and disciplined 230 more for violating the company's policies against pornographic eMail.
- The New York Times Company fired nearly two dozen employees and reprimanded another 20 workers for sending and/or receiving eMails that included sexual images and offensive jokes.

Social media experts said outright restrictions are rife with risk for most groups — not the least of which is being seen as a fuddy-duddy or a Luddite. These experts said a policy is essential, especially in a large organization, because any tweet is only a cell phone and a few seconds away.

Yet large local companies aren't all rushing to develop social media policies for their employees. Defense contractor Cubic Corp. doesn't have one. Sempra Energy has been working on one for six months and might finish it in another six.

Petco, the San Diego-based pet supply chain, adopted a three-page policy in November modeled after IBM's widely praised social computing protocol.

Petco intranet manager Daniel Sundin said the policy bars blogging and using social media at the office unless required as part of an employee's job. The policy says employees are personally liable for what they write and are precluded, in part, from sharing sales numbers and proprietary information or using the company logo without permission.

Although restrictions are needed, Sundin said, companies ignoring social media's power miss the big picture.

“That's just a head-in-the-sand thing, and you're a dying company if you're doing that.”

Ultimately, businesses and institutions have a simple choice, said Howard Rheingold, a self-described online instigator who teaches social media courses at Stanford University and the University of California Berkeley: Go with the flow or try to control it.

“Is there an advantage to having people see that we enable open communication, including criticism?” he asked. “Or do we think that there are some things that we ought to keep in the family?”

While that answer may depend on one's point of view, or job title, technology gurus agree that any hazards — from unveiling state secrets to mere embarrassment — decrease if the people using the technology understand how it works.

“If you don't know what you're doing, you could do all types of danger to your organization,” Rheingold said.

The types of Twitter trouble vary greatly.

Jurors' tweets triggered calls for mistrials in Arkansas and Pennsylvania in March. A renter was sued in July for \$50,000 for mentioning her Chicago landlord's name in a tweet about a moldy apartment. And media outlets from ESPN to *The Roanoke Times* have adopted social networking policies after staffers' tweets about news and company meetings made management wary.

Meanwhile, the Marine Corps banned the use of social media sites on government computers last month, and the military is considering wider restrictions even as recruiters acknowledge the tool's usefulness.

In sports, NBA player Charlie Villanueva was shamed into abandoning halftime tweets in March after his coach found fault with one that said he would step up in the second half. The Chargers fined cornerback Antonio Cromartie \$2,500 last month for a tongue-in-cheek post about what he called the team's "nasty" food at training camp.

Twitter's strength is its immediacy. Tweets are posted and read instantly by anyone with a computer or a cell phone, creating a collective consciousness and an organic, constantly evolving stream of information. Posts can be made private, but hardly anyone does it.

The popularity of Twitter has been explosive.

It started in San Francisco in early 2006, intended as a way for people to stay in touch with small groups of friends. Twitter's Web site eclipsed 1 million users in 2008. In June, it had 44.5 million visitors, according to Internet research firm ComScore Inc.

Companies from electronics retailer Best Buy to shoe seller Zappos have embraced Twitter as a way to communicate with consumers. News outlets, including *The San Diego Union-Tribune*, are increasingly doing the same; the CNN breaking news feed is among the most popular Twitter accounts.

Others with massive followings include actor Ashton Kutcher, who challenged and beat CNN to 1 million followers; Oprah Winfrey; President Barack Obama; and NBA star Shaquille O'Neal.

Sree Sreenivasan, a Columbia University digital journalism professor, cited O'Neal in making the point that any policies promoting "smarter, better, more thought-through uses of social media" need to be developed before people's tweeting habits take root.

"I think it'd be very hard for the NBA to say to Shaq, 'You can't tweet anymore,' □" Sreenivasan said.

Twitter enthusiast Becky Carroll, who teaches a new-media marketing class at the University of California San Diego, said many people might regard a Twitter ban as good for the military and bad for sports stars — which puts businesses like Petco in between, with a need for some restrictions in an area rich with marketing potential.

But she called a total shutdown "pretty un-American."

The very idea of information control is becoming an oxymoron, said Heather Honea, associate professor of marketing at San Diego State University. Still, she said, organizations are better off "helping develop the narrative" themselves.

“They're not going to manage the information entirely,” Honea said. “I just think they're going to manage who starts it.”

Social media experts said to remember one thing above all else when typing: Even short sentences can have long-lasting effects.

CNET executive editor Molly Wood joked online last month that Twitter lowers inhibitions and has an immediate effect, like alcohol. She called Twitter “the Long Island iced tea of the Internet.”

“Just don't tweet and drive,” she said. “That's not safe.”

## Sample Social Media Policies

### Casual/Humorous

In the spirit of Social Media, specifically Twitter, each sentence or paragraph of these guidelines will be 140 characters or less. [132]

When you use social media your actions, writing and content are not only a reflection of you but also the company you work for. [128]

There is only one Social Media guideline --> Use common sense! [63]

Seriously though, there is obviously some "fine print" involved with any guidelines or "rules of conduct." Social Media is no different. [137]

First, let's understand what is considered "Social Media." It's Blogs, Forums, Wikis and Social Networks and commenting therein. [129]

7 Social Media Do's - Be Polite, Be Courteous, Be Helpful, Be Conversational, Be Intelligent, Be Non-confrontational, Be Transparent [133]

7 Social Media Don'ts - Share Secrets, Curse, Bad Mouth, Complain about Company/Product, Act Stupid, Defame, Forget Day Job [123]

The Social Media Do's Explained [31]:

- Be Polite - Talk the way you would if you were doing a job interview. [72]
- Be Courteous - Be sure to listen & ask questions. [52]
- Be Helpful - Offering tips, tricks & how-to's goes a long way. [65]
- Be Conversational - Don't just be a PR twit. Chat as you would with a stranger at a bar. Be funny yet interesting. [117]
- Be Intelligent - Provide some value. Don't talk down. Offer insight. [71]
- Be Non-confrontational - Don't start a flame war, it can & will come back to haunt you. [90]
- Be Transparent - Disclose that you work for the company, be honest & truthful. [81]

The Social Media Don'ts Explained [33]

- Don't Share Secrets - If you aren't sure you can disclose something, just don't do it. [89]
- Don't Curse - If we find anyone cursing on Social Media sites, we will beat your \*&%#^ butt! [95]
- Don't Bad Mouth - Keep that mouth clean & avoid slamming people or companies. It helps you avoid a lawsuit or people hating you. [131]

- Don't Complain About Company/Product - Remember what your mom said: If you don't have anything nice to say, don't say anything at all! [137]
- Don't Act Stupid - Stupid is as stupid does. Think if your parents would be proud of your actions. [101]
- Don't Defame - Sometimes your competition can be your ally. Respect them professionally. [91]
- Don't Forget day job -Social Media can consume you so don't forget who pays your salary. If it doesn't help the company, be smart! [133]
- Most companies already have a Code of Conduct. Social Media should simply be considered another communication channel. [118]

If you don't know how you should act or communicate within Social Media, ask someone who does. Don't just do it blindly! [120]

Lastly, remember that people are listening. What you do on Social Media defines your personal brand! [100]

## **IBM Social Media Policy**

### **Introduction**

#### **Responsible engagement in innovation and dialogue**

Whether or not an IBMer chooses to create or participate in a blog, wiki, online social network or any other form of online publishing or discussion is his or her own decision. However, emerging online collaboration platforms are fundamentally changing the way IBMers work and engage with each other, clients and partners.

IBM is increasingly exploring how online discourse through social computing can empower IBMers as global professionals, innovators and citizens. These individual interactions represent a new model: not mass communications, but masses of communicators.

Therefore, it is very much in IBM's interest—and, we believe, in each IBMer's own—to be aware of and participate in this sphere of information, interaction and idea exchange:

**To learn:** As an innovation-based company, we believe in the importance of open exchange and learning—between IBM and its clients, and among the many constituents of our emerging business and societal ecosystem. The rapidly growing phenomenon of user-generated web content—blogging, social web-applications and networking—are emerging important arenas for that kind of engagement and learning.

**To contribute:** IBM—as a business, as an innovator and as a corporate citizen—makes important contributions to the world, to the future of business and technology, and to public dialogue on a broad range of societal issues. As our business activities increasingly

focus on the provision of transformational insight and high-value innovation - whether to business clients or those in the public, educational or health sectors—it becomes increasingly important for IBM and IBMers to share with the world the exciting things we're learning and doing, and to learn from others.

In 1997, IBM recommended that its employees get out onto the Internet—at a time when many companies were seeking to restrict their employees' Internet access. In 2005, the company made a strategic decision to embrace the blogosphere and to encourage IBMers to participate. We continue to advocate IBMers' responsible involvement today in this rapidly growing space of relationship, learning and collaboration.

### **IBM Social Computing Guidelines: Executive Summary**

1. Know and follow IBM's [Business Conduct Guidelines](#).
2. IBMers are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Be mindful that what you publish will be public for a long time—protect your privacy.
3. Identify yourself—name and, when relevant, role at IBM—when you discuss IBM or IBM-related matters. And write in the first person. You must make it clear that you are speaking for yourself and not on behalf of IBM.
4. If you publish content to any website outside of IBM and it has something to do with work you do or subjects associated with IBM, use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent IBM's positions, strategies or opinions."
5. Respect copyright, fair use and financial disclosure laws.
6. Don't provide IBM's or another's confidential or other proprietary information. Ask permission to publish or report on conversations that are meant to be private or internal to IBM.
7. Don't cite or reference clients, partners or suppliers without their approval. When you do make a reference, where possible link back to the source.
8. Respect your audience. Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in IBM's workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory—such as politics and religion.
9. Find out who else is blogging or publishing on the topic, and cite them.
10. Be aware of your association with IBM in online social networks. If you identify yourself as an IBMer, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and clients.
11. Don't pick fights, be the first to correct your own mistakes, and don't alter previous posts without indicating that you have done so.
12. Try to add value. Provide worthwhile information and perspective. IBM's brand is best represented by its people and what you publish may reflect on IBM's brand.

### **IBM Social Computing Guidelines: Detailed Discussion**

**The IBM Business Conduct Guidelines and laws provide the foundation for IBM's policies and guidelines for blogs and social computing.** The same principles and guidelines that apply to IBMers' activities in general, as found in the IBM Business Conduct Guidelines, apply to IBMers' activities online. This includes forms of online publishing and discussion, including blogs, wikis, file-sharing, user-generated video and audio, [virtual worlds](#)\* and social networks.

As outlined in the Business Conduct Guidelines, IBM fully respects the legal rights of our employees in all countries in which we operate. In general, what you do on your own time is your affair. However, activities in or outside of work that affect your IBM job performance, the performance of others, or IBM's business interests are a proper focus for company policy.

**IBM supports open dialogue and the exchange of ideas.** IBM regards blogs and other forms of online discourse as primarily a form of communication and relationship among individuals. When the company wishes to communicate publicly as a company—whether to the marketplace or to the general public—it has well established means to do so. Only those officially designated by IBM have the authorization to speak on behalf of the company.

However, IBM believes in dialogue among IBMers and with our partners, clients, members of the many communities in which we participate and the general public. Such dialogue is inherent in our business model of innovation, and in our commitment to the development of open standards. We believe that IBMers can both derive and provide important benefits from exchanges of perspective.

One of IBMers' core values is "trust and personal responsibility in all relationships." As a company, IBM trusts—and expects—IBMers to exercise personal responsibility whenever they participate in social media. This includes not violating the trust of those with whom they are engaging. IBMers should not use these media for covert marketing or public relations. If and when members of IBM's Communications, Marketing, Sales or other functions engaged in advocacy for the company have the authorization to participate in social media, they should identify themselves as such.

What does an IBMer's personal responsibility mean in online social media activities? Online social media enables individuals to share their insights, express their opinions and share information within the context of a globally distributed conversation. Each tool and medium has proper and improper uses. While IBM encourages all of its employees to join a global conversation, it is important for IBMers who choose to do so to understand what is recommended, expected and required when they discuss IBM-related topics, whether at work or on their own time.

**Know the IBM Business Conduct Guidelines.** If you have any confusion about whether you ought to publish something online, chances are the BCGs will resolve it. Pay particular attention to what the BCGs have to say about proprietary information, about avoiding misrepresentation and about competing in the field. If, after checking the

BCG's, you are still unclear as to the propriety of a post, it is best to refrain and seek the advice of management.

**Be who you are.** Some bloggers work anonymously, using pseudonyms or false screen names. IBM discourages that in blogs, wikis or other forms of online participation that relate to IBM, our business or issues with which the company is engaged. We believe in transparency and honesty. If you are blogging about your work for IBM, we encourage you to use your real name, be clear who you are, and identify that you work for IBM. Nothing gains you more notice in the online social media environment than honesty—or dishonesty. If you have a vested interest in something you are discussing, be the first to point it out. But also be smart about protecting yourself and your privacy. What you publish will be around for a long time, so consider the content carefully and also be judicious in disclosing personal details.

**Be thoughtful about how you present yourself in online social networks.** The lines between public and private, personal and professional are blurred in online social networks. By virtue of identifying yourself as an IBMer within a social network, you are now connected to your colleagues, managers and even IBM's clients. You should ensure that content associated with you is consistent with your work at IBM. If you have joined IBM recently, be sure to update your social profiles to reflect IBM's guidelines.

**Speak in the first person.** Use your own voice; bring your own personality to the forefront; say what is on your mind.

**Use a disclaimer.** Whether you publish to a blog or some other form of social media, make it clear that what you say there is representative of your views and opinions and not necessarily the views and opinions of IBM. At a minimum in your own blog, you should include the following standard disclaimer: "The postings on this site are my own and don't necessarily represent IBM's positions, strategies or opinions."

**Managers and executives take note:** This standard disclaimer does not by itself exempt IBM managers and executives from a special responsibility when blogging. By virtue of their position, they must consider whether personal thoughts they publish may be misunderstood as expressing IBM positions. And a manager should assume that his or her team will read what is written. A public blog is not the place to communicate IBM policies to IBM employees.

**Respect copyright and fair use laws.** For IBM's protection and well as your own, it is critical that you show proper respect for the laws governing copyright and fair use of copyrighted material owned by others, including IBM's own copyrights and brands. You should never quote more than short excerpts of someone else's work. And it is good general blogging practice to link to others' work. Keep in mind that laws will be different depending on where you live and work.

**Protecting confidential and proprietary information.** Social computing blurs many of the traditional boundaries between internal and external communications. Be thoughtful

about what you publish—particularly on external platforms. You must make sure you do not disclose or use IBM confidential or proprietary information or that of any other person or company in any online social computing platform. For example, ask permission before posting someone's picture in a social network or publishing in a blog a conversation that was meant to be private.

**IBM's business performance.** You must not comment on confidential IBM financial information such as IBM's future business performance, business plans, or prospects anywhere in world. This includes statements about an upcoming quarter or future periods or information about alliances, and applies to anyone including conversations with Wall Street analysts, press or other third parties (including friends). IBM policy is not to comment on rumors in any way. You should merely say, "no comment" to rumors. Do not deny or affirm them—or suggest either denial or affirmation in subtle ways.

**Protect IBM's clients, business partners and suppliers.** Clients, partners or suppliers should not be cited or obviously referenced without their approval. Externally, never identify a client, partner or supplier by name without permission and never discuss confidential details of a client engagement. Internal social computing platforms permit suppliers and business partners to participate so be sensitive to who will see your content. If a client hasn't given explicit permission for their name to be used, think carefully about the content you're going to publish on any internal social media and get the appropriate permission where necessary.

It is acceptable to discuss general details about kinds of projects and to use non-identifying pseudonyms for a client (e.g., Client 123) so long as the information provided does not make it easy for someone to identify the client or violate any non-disclosure or intellectual property agreements that may be in place with the client. Furthermore, your blog or online social network is not the place to conduct confidential business with a client.

**Respect your audience and your coworkers.** Remember that IBM is a global organization whose employees and clients reflect a diverse set of customs, values and points of view. Don't be afraid to be yourself, but do so respectfully. This includes not only the obvious (no ethnic slurs, personal insults, obscenity, etc.) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory—such as politics and religion. For example, if your blog is hosted on an IBM-owned property, avoid these topics and focus on subjects that are business-related. If your blog is self-hosted, use your best judgment and be sure to make it clear that the views and opinions expressed are yours alone and do not represent the official views of IBM. Further, blogs, wikis, virtual worlds, social networks, or other tools hosted outside of IBM's protected Intranet environment should not be used for internal communications among fellow employees. It is fine for IBMers to disagree, but please don't use your external blog or other online social media to air your differences in an inappropriate manner.

**Add value.** IBM's brand is best represented by its people and everything you publish reflects upon it. Blogs and social networks that are hosted on IBM-owned domains should be used in a way that adds value to IBM's business. If it helps you, your coworkers, our clients or our partners to do their jobs and solve problems; if it helps to improve knowledge or skills; if it contributes directly or indirectly to the improvement of IBM's products, processes and policies; if it builds a sense of community; or if it helps to promote IBM's Values, then it is adding value. Though not directly business-related, background information you choose to share about yourself, such as information about your family or personal interests, may be useful in helping establish a relationship between you and your readers, but it is entirely your choice whether to share this information.

**Don't pick fights.** When you see misrepresentations made about IBM by media, analysts or by other bloggers, you may certainly use your blog—or join someone else's—to point that out. Always do so with respect, stick to the facts and identify your appropriate affiliation to IBM. Also, if you speak about a competitor, you must make sure that what you say is factual and that it does not disparage the competitor. Avoid unnecessary or unproductive arguments. Brawls may earn traffic, but nobody wins in the end. Don't try to settle scores or goad competitors or others into inflammatory debates. Here and in other areas of public discussion, make sure that what you are saying is factually correct.

**Be the first to respond to your own mistakes.** If you make an error, be up front about your mistake and correct it quickly. In a blog, if you choose to modify an earlier post, make it clear that you have done so.

**Use your best judgment.** Remember that there are always consequences to what you publish. If you're about to publish something that makes you even the slightest bit uncomfortable, review the suggestions above and think about why that is. If you're still unsure, and it is related to IBM business, feel free to discuss it with your manager. Ultimately, however, you have sole responsibility for what you post to your blog or publish in any form of online social media.

**Don't forget your day job.** You should make sure that your online activities do not interfere with your job or commitments to customers.

---

<sup>1</sup> Number of members provided by Facebook.com

<sup>2</sup> For monthly visits (for all social media in this report) - Compete.com – January 2009

<sup>3</sup> For average page views & average time user spends (for all social media in this report) – Alexa.com, 3-month average, September 30, 2009

<sup>4</sup> Wikipedia.com

<sup>5</sup> Answers.com

<sup>6</sup> Alexa.com

<sup>7</sup> Mashable.com

<sup>8</sup> Data directly from LinkedIn.com (September 30, 2009)

- 
- <sup>9</sup> Blogcatalog.com
- <sup>10</sup> Salary.com & AOL Survey – July 11, 2005
- <sup>11</sup> Kelleher, David. Social Networking at Work. IT World, February 23, 2009
- <sup>12</sup> Proofpoint. Employer Survey, August 2009
- <sup>13</sup> CareerBuilder.com
- <sup>14</sup> <http://www.privacyrights.org/fs/fs16b-smallbus.htm>
- <sup>15</sup> Careerbuilder.com survey. June, 2009
- <sup>16</sup> Blakeley, Kiris. Forbes Magazine. August 11, 2009
- <sup>17</sup> Society of Corporate Compliance & Ethics. Survey, August 2009
- <sup>18</sup> Hrhero.com, Why Employers Can't Ignore Social Networking Sites, September 11, 2009
- <sup>19</sup> Leonard, Matt. Why Employees Need Social Media Guidelines. Search Engine Journal, August 19, 2009
- <sup>20</sup> Deloitte LLP 2009 Ethics & Workplace Survey