

Is your business cyber-savvy? The essentials of an ‘acceptable use’ policy

Businesses whose employees do not master the potentials of the Web will quickly be overcome by more nimble and aggressive competitors... But employee access to Internet applications poses a number of risks which must be effectively managed

The Internet is a ubiquitous business tool, essential for e-mail, research, communications, networking, news and information. These are all dynamic and essential functions, and businesses whose employees do not master the potentials of Web 2.0 will quickly be overcome by more nimble and aggressive competitors.

Yet employee access to internet applications poses a number of risks which must be effectively

If [defamatory] comments are made using the employer’s systems in the course of the employee’s employment, the injured party inevitably will argue that the employee was acting as the company’s agent and the company is therefore legally liable for the defamatory statements. Employees need to be trained to make business communications, particularly those which easily can be forwarded to third parties, appropriate and measured in tone and content.

managed. Threats include loss of productivity and distraction, invasion or loss of privacy, copyright violations, defamatory communications—even predatory behavior. The company adopting best practices will manage these risks through a thoughtfully constructed

acceptable-use policy.

It’s fundamental that businesses determine if it is beneficial to encourage or prohibit employees from using networking

Web sites. Facebook, LinkedIn, Blogger and similar sites are attracting millions of people who understand the potential of social and business networking. Research firm Forrester estimates that businesses will spend more than \$250 million this year on social networking sites geared toward their business models. But if employees spend their days posting weekend party photographs on their Facebook page, and do not have a clear and focused business plan for using networking sites, they are squandering

their employer’s time and resources during an economic period which is not tolerant of waste. Training and appropriate policies are the vehicles for using these tools well and not wantonly.

The effective acceptable-use policy should focus on creating



R. Craig Wood
Guest Columnist

clear and easy-to-follow guidelines for employees to follow. It should inform employees which applications and Web sites are appropriate to access during the business day, and which are not, at least in a general sense. It should encourage appropriate business activities, discourage purely personal activities such as second job pursuit, and outright prohibit access to pornographic Web sites and material. It should explain legal risks such as copyright laws, and assist employees by helping them avoid inadvertent violations.

Employees have a privacy expectation in their e-mails, but employers have a competing interest in ensuring that company e-mail systems are not being used for inappropriate purposes. The range of activities that may be considered “inappropriate” is impossible to catalog in a brief article, but range from threatening e-mails, to disclosure of confidential business information to third parties, to e-mails containing sexual or defamatory content. The individual’s right not to have someone reading her e-mail is codified in the Electronics Communications Privacy Act (ECPA), a federal law passed in 1998. The ECPA makes it a federal crime for an individual to intercept, access, disclose or use another’s wire or electronic communications, which would include e-mails, unless the individual consents to the access. The employer can overcome the expectation of privacy by making company access to employee e-mails a condition of use of the employer’s com-

puter system. The consent of the employee is implied because the employee uses the employer’s system after having been informed in writing that the employer reserves the right to monitor such communications. Employees can still maintain personal e-mail accounts, but use of these personal accounts for business purposes should be prohibited. Any business e-mails should be subject to review by the employer in the same manner as any other business document, correspondence or record. The utility of a good acceptable use policy is evident—what is a serious violation of federal law can be turned into a proper exercise of employer authority simply by following a basic set of legal guidelines. This is where the company working with competent employment-law counsel is an excellent investment of modest resources.

One of the ways employers may be held liable for employee conduct in electronic communications is when the employee defames someone. Defamation is generally defined as a false statement that impugns someone’s character or professional qualifications made to a third party. Employees who use language carelessly when criticizing someone’s integrity or job performance can be guilty of defamation. If the comments are made using the employer’s systems in the course of the employee’s employment, the injured party inevitably will argue that the employee was acting as the company’s agent and the company is therefore legally liable for the defamatory state-

ments. Employees need to be trained to make business communications, particularly those which easily can be forwarded to third parties, appropriate and measured in tone and content.

Finally, employers need to anticipate that one or more of their employees may use the employer's electronic systems for very inappropriate or even illegal purposes. Sexual content is easily accessible on the Internet, and if one employee shares sexual content to another who finds it embarrassing or offensive, then the employer can be liable under federal and states laws that prohibit sexual discrimination and harassment. Sexual predators commonly use social networking Web sites to attract and pursue their victims. The extent of that activity is staggering. For instance, the youth-oriented Web site MySpace was recently criticized in the media for not taking sufficient measures to protect children from sexual predators. By late January 2009 FoxNews reported that MySpace had found more than 29,000 registered sex offenders with profiles on the popular Web site, more than four times the number cited by the company just two months earlier. Then on Feb. 4, CNN.com reported that "MySpace.com has identified and removed 90,000 convicted sex offenders from its popular social-networking site, according to one of the dozens of state attorneys general who pressured the site to beef up its safety standards." One must wonder if the number of identified registered sex offenders ballooned from around 7,000 to 90,000 in less than two weeks, whether the Web site is really on top of the problem. Even if it is, the number represents only "registered sex offenders"—in other words people who have been caught and convicted of sex crimes—and is nowhere near an accurate approximation of the number of sexual predators who are active but have escaped prosecution and conviction so far. Employers must not

underestimate the extreme damage that will be done to their personal and corporate reputations if one of their employees is charged with sexually predatory behavior, and it is revealed that the conduct was being carried on at least in part at work, and the employer was oblivious to it and did nothing to detect or prevent it.

Web 2.0 offers tremendous opportunities to companies and their employees to expand their business models and increase their

efficiency and profitability. But it also presents significant legal risks which must be identified and managed through appropriate policies and electronic screening tools. Companies need to work with legal counsel who are knowledgeable not only about federal and state employment laws, but also about the laws and regulations and risks of the cyber world. Good preventive practices can prevent a myriad of legal claims and eliminate legal

and reputational threats that could cripple or destroy your business.

(R. Craig Wood is the managing partner of the Charlottesville office of McGuireWoods LLP, an international law firm headquartered in Richmond. Wood regularly represents employers on legal issues and lawsuits in central and western Virginia, and is a frequent author and lecturer on litigation and employment law topics. The firm and Wood can be found on the Web at www.mcguirewoods.com)

bankruptcy & creditors' rights | construction | corporate | environmental | estate planning
family law | health law | intellectual property | labor & employment | litigation
local government | real estate & land use | regulated industries | tax

Choosing a law firm is a lot like buying a diamond.



Everyone seems to focus on just one of the four Cs. But look further and you'll realize there is more to the selection than just size. Our attorneys concentrate on personal service that's a cut above what a global mega-firm can offer. And with specialists in most major practice areas, we can bring clarity to almost any matter – at a cost the big city firms can't touch. Call us today to see how we practice the most important quality of all: commitment.



woodsrogers.com | 800 562-4629

ROANOKE | DANVILLE | BLACKSBURG | LYNCHBURG | RICHMOND

Authorized by Michael C. Carr, Chairman, on behalf of the firm.