

It's 10:00 a.m. —
Do you know what your employees are doing?
Everybody's gone surfin' during the business day

According to a study in a recent *U.S. News and World Report* article, American employees are spending up to two hours each business day surfing the internet conducting non work-related activities. Internet access on employer-provided computers is intended to increase productivity and efficiency. Although there are many legitimate business related uses of the internet such as the ability to find detailed, up to the minute information with ease, it is just easy to find other diversions online. With internet access just a click away, some employees think that it is perfectly acceptable to review personal email, perform online banking, check stock quotes, shop, or even look for other jobs – all on company time. Unauthorized “cybersurfing” is becoming a financial drain for many businesses and it may consequently render employers legally vulnerable to the online activities of their employees.

Does your company have an internet policy? And, even if you do, are you prepared to enforce it? Companies have many valid reasons to monitor what their employees are doing on business computers in an effort protect privileged information or to prevent sexual or racial harassment for example. The temptation of internet access is such a strong distraction, however, that some employees will continue to cybersurf despite company guidelines. Some are even bold enough to check online bets or even visit pornographic or racist websites exposing their employers meanwhile to liability by these precarious activities. Employees will continue to use business computers for their own purposes even at the risk of their own privacy if they do not suffer any consequences for their actions. Employers must be willing to reprimand or even fire employees who engage inappropriate internet use. In addition, employers may have added responsibilities with regard to the internet use of their employees if any illegal activities are discovered. If employers are made aware of such conduct on business computers, employers themselves may be held accountable if the misconduct is not reported to authorities.

Consider the recent New Jersey case of *Doe v. XYZ Corp.* where an employee was using a workplace computer to send nude photographs of his ten year old step daughter to child pornographic websites. Despite the fact that this criminal activity was taking place at the office, his immediate supervisor, even after being notified repeatedly, chose not inform senior level management. The employee's wife sued the company on behalf of her young child alleging that the company, despite their knowledge of this unfortunate, ongoing situation, did not take the steps necessary to protect her child and for their failure to report the abuse to law enforcement authorities. In its decision, the New Jersey intermediate appellate court held that the employer, by not investigating the matter and taking proper action, resulted in liability for injuries to a third party stating, “An employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a **duty** to investigate the employee's activities and to take prompt and effective

action to stop the unauthorized activity, lest it result in harm to innocent third-parties. No privacy interest of the employee stands in the way of this duty on the part of the employer.” The impact of this decision broadens the responsibility of the employer with regard to investigating and curtailing inappropriate internet use. With this case in mind, employers must step beyond the boundaries of the company, and report illegal conduct, particularly when it involves child pornography.

So what should an employer do in order protect themselves? As part of an overall internet policy, Kim Komando, host of the nation’s largest talk radio show about computers and the internet suggests, “Make all employees sign a computing policy on their first day of work. This way they know that you mean business and that the computers and internet access lines are intended to further the company’s goals.” Courts have given employers considerable latitude as to what happens on their computers and rulings have even upheld the reading of the emails by employers as long as they sent on company owned computers. If employees know that their computer use at the office will be monitored, they should not expect any privacy.

The best way for employers to address computer use at the office is to implement a clear policy outlining the permissible parameters of employee internet use, or an Internet Acceptable Use Policy (IAUP). An IAUP is a written agreement, signed by employees, which outlines company rules for acceptable workplace uses of the internet. An IAUP, by extension, must set out a policy pertaining to prohibited internet uses, rules of online behavior, and access privileges. Penalties for violations of the policy, including security violations and vandalism of the system, should also be covered. Anyone using a company’s internet connection should be required to sign an IAUP, preferably on their first day of employment, and know that it will be kept on file as a legal, binding document.

When creating an IAUP for your company or organization, you should consider, for example, the following:

- Whether employees are allowed to browse the web for personal use as well as business purposes
- When employees can use the web for personal use
- If and how the company monitors web use and what level of privacy employees can expect
- Web activity that is not allowed. Review unacceptable behavior in detail

Provide two copies of the policy to employees - one for them to keep and another for them to sign and return to you.

Employers, in essence, have multiple responsibilities with regard to internet access. In most instances, internet access at the office is used the way in which it was intended - to enhance employee productivity and job efficiency. Without any guidelines in place, internet access on the part of employees can get out of control, and in some instances, with serious ramifications. Since many employers have recognized that unrestricted use of the internet is unwise, many have adopted or in the process of implementing an Internet Acceptable Use Policy. Without one, you may wind up in a “web” of trouble.

If you would like any additional information, please contact us at the Katz Law Group, P.C.