

By Bill Boothe

Monitoring Employee E-mail & Internet Usage

When it comes to monitoring your employees' use of club e-mail and the Internet, your rights as an employer are pretty clear. If your club owns the equipment, your club generally has the right to monitor your employees' activity.

But while most employers emerge victorious from lawsuits over monitoring, careful planning and good communication are still your best bets for avoiding legal action altogether – and not alienating your employees.

In its most recent survey of workplace monitoring and surveillance, the American Management Association (AMA) found nearly 78 percent of all major U.S. firms recorded and reviewed employee communications and activities on the job in 2003, including phone calls, e-mail, Internet connections and computer files. That figure is double the number of just four years earlier.

Why monitor your employees?

The reasons employers monitor their employees' communications range from ensuring legal compliance, to increasing worker productivity, to documenting employee performance for review, to security and protection from liability. Regulated industries like those in the financial sector report the highest level of employee monitoring of all kinds – 95 percent, according to the AMA. Unfortunately, not monitoring employee communications can also leave companies vulnerable. For example, employees who are exposed to offensive graphic material on a co-worker's computer screen could file a lawsuit based on discrimination, harassment or operating in a "hostile workplace environment."

How and what to monitor

Although the law favors the employer in workplace monitoring cases, the laws governing such practices are in a constant state of flux because the technologies are new and continually evolving. Experts agree that the best way to protect your club from a lawsuit is to clearly spell out your monitoring policy in your club's employee handbook. The following are a few general guidelines for monitoring different types of activities:

E-mail: Employers generally have the right to monitor an employee's incoming and outgoing e-mail. A 2003 AMA survey found that more than half of U.S. companies engage in some form of e-mail monitoring of employees. But while three-quarters of those surveyed say their organization has written policies concerning e-mail, fewer than half train their employees on them.

Internet: While the Internet brings with it countless oppor-

tunities for increased productivity and communication, it also brings easy access to graphic sexual images, on-line gambling and other material inappropriate for the workplace. Employers can choose to install monitoring systems that will block specific sites, alert administrators when employees try to access an inappropriate page or maintain logs about which sites each employee accessed and for how long.

Computer Files/Computer Use: Besides having the right – as well as the legal responsibility – to monitor employees' downloaded files, installed applications and computer files for security and propriety, employers can also install devices that let them monitor every keystroke an employee makes for productivity and other information tracking. While legal as part of a communicated policy, employers should weigh the business need against the risks of alienating their employees with Big Brother-like tactics.

PDAs: Although virtual offices, mobile employees and ever-shrinking communication technologies may make monitoring some devices more problematic, the general rule is, if the club owns the equipment and the employee is being paid by the club, then the club has the right to monitor activity.

Communication is key

Perhaps as important as having a detailed workplace monitoring policy is a plan to communicate the policy to your employees. Some tips include:

- Make sure your employees know how they are being monitored - and why they are being monitored.
- Be clear with your employees about what you will, or will not, monitor. Although some recent court decisions have supported employers who snooped when they said they wouldn't, such practices can create a negative work environment and can pose a greater threat to workplace productivity.
- Distribute the policy in writing and have employees sign off on its content.
- Train your managers and supervisors to recognize when communication tools are being misused.
- Be reasonable about what constitutes "infringement." Oppressive workplace monitoring will foster employee ill will and can create retention problems.
- Enforce your policies equally throughout the club. **BR**

Bill Boothe is director of club/resort technology consulting for RSM McGladrey, Inc. one of the nation's largest business services providers. Bill is the author of the national newsletter Private Club Technology Update. He can be reached at (561) 682-1638, via e-mail: bill.boothe@rsmi.com or at www.rsmmcladrey.com/privateclubs.