

Ethics Online: What A Good Internet Policy Looks Like

[Published in Compliance Week 06/12/2007]

You are meeting with the CEO in her office when the IT director comes in with a big grin on his face. "This new e-mail monitoring system is great!" he says. "You'll never guess who's having an affair."

The CEO takes the high road and tells him she doesn't want to know any more, and that the system is supposed to be used to make sure employees are being productive and not doing things that create legal or resource problems.

"So," he smirks "I guess that means you don't want to know who has choice words to describe you, either." The CEO shakes her head.

"Too bad you didn't want to know, especially since he's been posting our formulas on his blog," quips the director as he exits the room, log files clutched in hand.

The CEO turns and looks at you, the compliance and ethics officer, for advice. Yikes, you think, none of my legal or ethics training prepared me for this!

* * *

E-mail and Internet usage—not to mention newer technologies such as blogs and news feeds—have quickly become technological requirements in today's business world. Policy and corporate practice, however, has not always kept up with technology, especially in managing e-mail and Internet files. The Electronic Discovery Act that took effect late last year confirmed what many executives have already been learning on the job: If a company provides e-mail accounts and Internet access for employees, it had better also have a plan defining their use, monitoring and storage. Failure to do so can create a bevy of problems from legal liability to invasion of employee privacy and trust.

Technologically, accessing the outside world for any purpose can open up corporate computer systems to the risk of viruses and spyware, but personal use can exacerbate the problem if it is not approved or controlled by the IT department. Legally, personal use of technology opens up a Pandora's box of potential corporate liability. In fact, the American Management Association's 2005 Electronic Monitoring and Surveillance survey found that one in five

employers has had e-mail subpoenaed by courts and regulators, and another 13 percent have defended lawsuits triggered by employee e-mail.

Ethically, use of technology can be its own slippery slope, unless employees know what acceptable use looks like. Eighty-seven percent of individuals access the Internet for personal use at work, but it is those who abuse the privilege who cause the greatest harm. If a company knows and does nothing about flagrant overuse, it affects not only that employee's productivity, but also creates a climate that accepts misuse. Inappropriate or ill-considered statements made by employees in e-mails, blogs and instant messages can become smoking guns for the erosion of public trust, not to mention the other side in lawsuits or investigations: just ask Enron, Boeing or Hewlett-Packard.

The Ethics of Electronic Privacy

Although it is clear that a company has the right to monitor employee use of company-supplied e-mail accounts and Internet access, the ethical questions surrounding employee privacy are not as easy to answer. On the one hand, companies can easily lose control over employees' dedicated work time or the flow of proprietary information if they fail to monitor and control e-mail communications. On the other hand, there are many ethics-based reasons to allow unfettered access to the Internet. These include:

- **Productivity:** Employees can spend more time at work if they feel connected to their private lives and can accomplish some tasks without ever leaving their desks.
- **Professional development:** Employees who use technology for personal reasons often transfer those skills to their work. In addition, they may be better informed about current events or industry trends.
- **Psychological benefits:** Employees need breaks and downtime; e-mailing a friend or shopping online creates a quick psychological break, much like going out for coffee or taking a walk around the block.
- **Employee benefits:** Many employees consider personal use of e-mail and Internet access a perquisite, similar to having a company phone or privileges at the company fitness center. According to a 2006 Websense survey, half of those that said they use the Internet at work for personal reasons would rather give up their morning coffee than the ability to use the Internet at work for personal use.

So long as the employee complies with policy and does not overburden bandwidth, Internet usage is a fairly simple and costless benefit to provide. The key is to find a middle ground between potential risk and personal use—and to adopt that as a corporate Acceptable Use Policy (AUP).

Developing and Enforcing an Ethical Use Policy

An AUP, like any company policy, should mesh with corporate structure, company values, organizational culture and other existing policies, including equal employment opportunity, discrimination and harassment, communications, and security. A well-developed policy that is justified by business requirements and sets the tone from the top by being consistently and fairly applied will be much more readily accepted and obeyed by employees. Here are some steps to follow:

Get employee buy-in and feedback. Seek input from all departments, legal counsel and employee representatives. Do a baseline study to find out how employees use technology for personal reasons; analyze that in terms of company values, goals, and culture.

Make sure your policy satisfies or enhances the company's values and mission. Cite organizational values in the preamble explaining the need and goal of the policy. Creating a policy without considering the corporate culture can result in resentment, mistrust and impaired productivity.

Explain the "do's" and the "don'ts." Tell employees what appropriate conduct looks like, in addition to what is prohibited. Be specific about what types of sites and searches are allowed (say, shopping and news sites) or prohibited (pornography or gambling). On the other hand, define "systems" and "use" broadly enough to encompass new technologies. Remind employees they should not say anything in e-mail that they would not put on paper, should not access Web sites that they wouldn't want the boss to see, and should not use corporate resources or e-mails to say or do things that reflect negatively on the company.

Communicate trust, but reserve the right to monitor, access and store Internet, e-mail, and computer files. Make it clear in your policy that you trust them, but they should also have no expectation of privacy in email communications or Internet access when using company equipment.

Explain the legitimate business reasons for monitoring. Employees will be less likely to rebel if they know the purpose of monitoring is preserve company resources and protect the company from liability as opposed to eavesdropping on personal communications.

List potential disciplinary actions. Those actions should include oral and written warnings, as well as firing if there is constant abuse or illegal conduct. Make sure employees know they and the company can be subject to regulatory sanctions and civil and criminal liability for certain activities. Reserve the right to withdraw e-mail accounts or Internet access.

Next Steps

Once a policy is developed, be transparent about company processes related to monitoring of Internet use. Disclose in advance whether and how the company will be monitoring electronic communications. Consider including a statement on outgoing e-mails that says electronic communications are monitored and that the company is not liable for individual misuse. Provide a way for recipients to contact the company if they receive inappropriate e-mails.

Even further, select the least invasive but still effective monitoring software and systems. Even if they know monitoring occurs, employees may still resent the practice if they feel it is overly invasive or restrictive. Select software that automatically flags problems without requiring a human to read through hundreds of non-damaging personal e-mails.

Finally, do as you say and enforce the policy. Failure to investigate violations and to issue discipline accordingly not only creates evidence that the company knew about illegal or offensive behavior and failed to act, it can also erode employee confidence and trust. Without trust, an ethical culture is impossible to maintain.

AMA survey: Electronic Monitoring and Surveillance 2005
http://www.amanet.org/research/pdfs/EMS_summary05.pdf

2006 Web@Work study, conducted by Harris Interactive® for Websense
http://www.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork/Employee_Computing.pdf (survey results)

Article on 2005 AOL/Survey.com on wasting time at work
<http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2005/07/11/wastingtime.TMP>
http://www.websense.com/docs/InternetAccessPolicies/IAP_Stan.doc

