A Common Sense Guide to an Internet Use Policy

Apr 01 1999

Practice Area: Labor and Employment

For a number of years, technology has been a hot topic for most lawyers, from solo practitioners to members of very large firms. At the forefront of many legal technology seminars are issues relating to the use of the Internet as a legal and nonlegal information resource. One issue growing in importance involves establishing an employer's Internet use policy. This article will suggest a common sense approach to establishing an employer's policy governing Internet usage that is designed to permit some incidental personal use, but protect against the negative aspects of inappropriate Internet use.

OPTIONS FOR AN INTERNET USE POLICY

As a practical matter, there are four basic options for an employer's policy regarding Internet use by employees:

- **Don't provide the resource to employees, and prohibit Internet access at work and during work hours.** While reasonable minds may differ, many experts believe this option does not make business sense. In the Information Age, business success is more and more dependent on the ability to quickly access and process information. In addition, the proper use of technology helps to level the playing field for small companies faced with increasing competition from larger concerns.
- **Provide the resource, but don't regulate its use.** This option makes even less business sense than the option of not providing the resource at all. Inappropriate Internet use can adversely affect an employer's business, interfere with the work of its employees, increase its costs, and expose the company to liability.
- **Provide the resource, but limit its use to solely business-related purposes.** This is a reasonable alternative to the first two options, and some employers have adopted such a policy. However, while technologically viable, the resources required to monitor and effectively enforce policy can make it a financially burdensome option.
- **Provide the resource primarily as a business tool, but permit incidental personal use.** The basic premise for any Internet policy should be that Internet access provided by an employer is intended primarily as a tool to help the company better serve its customers. However, some incidental personal use of the Internet is likely to improve employee morale, increase employee productivity, and cement employee loyalty. Within that framework, common sense should dictate when incidental personal use of the Internet or Internet e-mail is appropriate, both as to the frequency of such conduct, and the nature of the use to which the Internet or e-mail is put.

What follows are suggested points to be included in such a policy. The suggestions are not meant to be exhaustive.

COMPONENTS OF A COMMON SENSE INTERNET USE POLICY

• **Integrate the Internet use policy with other existing policies.** Since there are other resources, such as telephones, which employers have provided employees for years, a company's Internet policy does not have to be viewed as an entirely "new" policy. It can instead be modeled after current policies governing the personal use of those other resources during work hours. For example, just as an employer would not reasonably be expected to tolerate hour-long personal telephone calls, the employer would not reasonably be expected to condone hours spent for personal enjoyment on the Internet during working hours.

As will be discussed in greater detail below, the Internet use policy should be coordinated with other pre-existing employment policies such as the prohibition of sexual harassment in the workplace, and the rules governing privacy in the workplace.

• **The Internet Use Policy should stress that incidental personal use is a privilege, which can be lost through abuse.** The Internet policy should stress that employer-provided Internet access is a privilege and not a right. The policy could acknowledge that, while Internet access is primarily a business tool, the employer recognizes and accepts the fact that there will be incidental personal use of the Internet just as there is personal use of the telephone. The policy should make a clear statement to the employee that Internet use will be monitored and, if the privilege is abused, the privilege will be lost by reason of such abuse. The Internet policy should be tailored to avoid or eliminate potential abuses of the Internet and establishing guidelines and/or examples of what are considered to be acceptable and unacceptable uses of the Internet can help meet this objective.

• **Employees should be informed that when they go online at the office, their actions might be identified as those of the employer.** This is particularly true for e-mail, since business e-mail addresses typically identify the organization in some manner. For example, as noted at the conclusion of this article, the author's e-mail address includes the employer's name. In such instances, therefore, the policy should advise employees that when using the employer's Internet e-mail system, the employer is normally identified in the e-mail. It is therefore impossible for employees to send e-mail without associating themselves with their employer.

Also, the consequences of that association should be clearly spelled out. The policy should set forth forth in plain English that what they say and what they believe to be personal statements could very well be attributed to the employer and that the employer may be held responsible for their conduct.

• **Employees should be informed that sending e-mail over the Internet is instantaneous and generally nonretrievable.** Employees should be made aware that drafting and sending e-mail is not like sending a letter. Unlike a letter, which may be retrieved from the mailroom, the e-mail is instantaneously sent from the computer station, and you cannot get it back for editing, or stop it from reaching its destination. It simply cannot be recovered, even if misdirected.

• **Employees should be informed that they lose a degree of privacy when they use the Internet or send e-mail over the Internet through the employer.** The employer should advise the employee both in its Internet policy and in a policy dealing with more general workplace privacy issues that e-mail sent from the office should not be considered private communication. Such a clear statement can act as a defense to an invasion of privacy claim in the event a personal e-mail is read by others whom the sender did not intend to read it. An employee who was clearly advised that the e-mail is not to be in any way considered private would not have a reasonable expectation of privacy when others receive or have access to the e-mail message.

Employees also should be told in the Internet use policy that they run the risk of giving up privacy protection just by sending e-mail. While hacking or stealing Internet e-mail messages is illegal, it is technologically possible for an individual to intercept and read an e-mail message. Employees should understand, therefore, that there is this potential loss of privacy. A common sense guideline for illustrating this for employees is that they should understand that the Internet email is very similar to writing on the back of a postcard.

Finally, employees should be advised that in many instances the technology creates a record of their Internet activities. For example, it is currently possible in at least a limited way to retrace the sites visited by an employee. It is also possible to monitor e-mail activity.

• **The policy should deal with issues of security.** The question of security has two aspects. The first involves the security and protection of the company computers. The company policy should address the issue of computer viruses, and establish procedures for opening e-mail attachments and downloading off the Internet.

Second, the policy should focus on the use of e-mail security such as passwords or encryption. An Internet e-mail policy should address the issue of when, if ever, an employee can encrypt personal e-mail. In addition, the policy should state that passwords or encryption keys must be made available to the employer so that the employer can have access at any time.

This is another area where reference to policies involving existing resources may be helpful in illustrating the purpose for this policy. Employers frequently have a policy relating to a right of access to an employee's desk or file cabinet. The Internet policy should provide that just as the employer has a right of access to the employee's desk or file cabinet, the employer will have access to the employee's computer and e-mail messages.

• **The Internet use policy should focus on excessive or inappropriate use.** There are a number of activities that should be expressly prohibited in every e-mail or Internet use policy, including the following:

- Copying, disseminating or printing copyrighted materials. This can include articles, images, games, or other software.
- Accessing, sending, soliciting, displaying, printing, or otherwise disseminating material that is reasonably likely to harass, threaten or embarrass others or that is sexually explicit, fraudulent or otherwise inappropriate in a professional environment.
- Transmitting statements, language, images or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
- Engaging in personal, non-employer related activities for gain or profit. Examples include consulting for pay or advertising or selling goods or services for personal gain.
- Engaging in illegal activities or using the Internet for any illegal purposes, including initiating or receiving communications that violate any laws or regulations.
- Interfering with or disrupting the work of others.
- Gaining or improperly gaining access to the Internet by using any access control mechanism not assigned to the particular user, or permitting another person to have access to the Internet by using the employee's access control mechanism.
- Hacking. Hacking means gaining or attempting to gain the unauthorized access to any computers, computer networks, databases, data or electronically stored information.

In addition, the policy should state that excessive personal use of the employer's e-mail or Internet resource will lead to loss of the privilege to use them. What is "excessive" may be difficult to define with precision. However, the most obvious excessive use is when work is suffering as a result. A further method of controlling excessive use is to incorporate a progressive discipline procedure with regard to what the employer considers to be excessive use, and the progressive discipline will then provide the employee with ample warning as to the employer's expectations.

The employer should also be flexible in its policy on excessive use. At certain times the personal use of the e-mail may far exceed normal personal use. For example, if the home team has won the Super Bowl, one could expect that Monday morning will generate a larger than normal e-mail transmission dealing with nothing other than the results of the Super Bowl contest. Again, common sense would dictate that this would not be the appropriate time to crack down on the personal use of the Internet, but rather for a reasonable employer to recognize that certain extraordinary events result in extraordinary usage of the e-mail system.

As noted above, the policy should be aimed at avoiding offensive language or activities that might be considered offensive to a reasonable person. This is particularly true of e-mail use. This offensive conduct could involve the choice of language, improper or inappropriate jokes, or the harassment "teasing" of a particular individual of the employer.

It is important that the policy inform the employees that if they are subjected to e-mail transmissions which involve improper language, jokes or harassing behavior, they have the ability to report that activity to management and that swift and appropriate actions will be undertaken to stop such offensive conduct. Again, it is recommended that the e-mail policy be cross-referenced or perhaps even incorporate portions of the employer's sexual harassment policy in order to underscore the importance of these prohibitions against improper use.
