



Risk Insights

Employee Internet Usage at Work: What They View Can Hurt You

For employees who spend their days working on a computer, the Internet is a valuable, indispensable resource. However, it can also create significant liability problems for the company, not to mention diminished productivity resulting from personal business being conducted on company computers. Therefore, it is essential for employers to have clear, specific Internet usage policies that are widely communicated and consistently enforced.

Legal Liability

Because the company owns the computers that employees work on, the company can legally be held liable for any illegal or discriminatory content that employees view or distribute on those computers.

Discrimination/Harassment

One concern is discrimination and sexual harassment. This can result from an employee sending inappropriate or offensive e-mails, or from an employee viewing pornography, other sexually explicit material, or content that promotes hate and discrimination. Even if the individual is not distributing such inappropriate content, an employee walking by could be offended and sue the company for being subjected to a hostile work environment.

Illegal Activity

Another legal liability for employers is any computer activity that involves or leads to illegal activity. This can include accessing illegal information, participating in illegal activities online, or using information found online to commit a crime. In addition, child pornography is of particular concern for employers, both because of the severity of the crime and because studies show that many people who view such content do so during work hours.

In any of the above cases, even if the employer was unaware of the inappropriate or illegal computer activity, it can be liable for negligent supervision of employees. Legally, any content stored on the computer is technically both in the employee's and employer's "possession."

Misuse of Company E-mail

Another type of legal liability could result from improper use of company e-mail. For example, if an employee sends personal e-mail from his/her company account or uses his/her company e-mail address to identify themselves in a chat room or Web site, then the company is liable for any statements made or actions performed. This could bring up issues of defamation, discrimination or links to illegal activity simply by the employee misusing a company e-mail account.

Technological Risks

Accessing unauthorized Web pages can also pose risks to the company's computer or network. Just one click of the mouse can expose a computer to a destructive virus or allow a predator access to sensitive company information.

Drain on Productivity

Studies have revealed that employees often spend large amounts of time "surfing" the Web or conducting personal business on the computer during work hours. While incidental personal use is understandable, more than that can be a significant drain on your company's resources by paying employees who are not consistently working.

Costs of Liability

There can be significant costs, financial and otherwise, associated with claims of computer or Internet abuse by employees. Lawsuits and settlements can be extremely costly to the company, whether it be for discrimination, harassment or illicit activity. In addition, dismissing employees guilty of misconduct can be expensive and time-consuming, both in finding and training a

replacement, and in potential legal fees if there is a legal dispute as a result.

The effect on other employees can be substantial as well. If it is a case involving discrimination or harassment, affected employees can become disenfranchised with the company itself, even if the company did nothing wrong and had a swift, appropriate response. Also, the company can suffer from a damaged reputation from the incident, and its name may become linked in people's minds as associated with the incident.

Protecting the Company

Employee Computer Usage Policy

The first step for employers to protect the company is to have a thorough, specific and well-communicated "Employee Computer Usage Policy." Not only can such a policy help prevent improper or illegal computer activity by employees, it will also go far to protect the company in the event of an investigation or lawsuit.

The policy should emphasize that the employees are using company property and that there is no reasonable expectation of privacy when working on company equipment. This extends to all Web sites visited and e-mails sent or received. The policy should make clear that the company "owns" the employee's e-mails and that they can be viewed at any time and/or used against the employee in future legal proceedings.

It is also vital that the policy spell out what the company deems as inappropriate use: hate, discrimination, harassment, child pornography, illegal content, sexually illicit content, etc. In addition, it should explain the consequences for abusing computer usage privileges or failure to follow any portion of the policy.

Employee Education

In addition to crafting such a policy, employees need to be fully aware of it. Employers should ask all employees to sign the policy, and then employees should retain a copy so that they are always aware of the policy and consequences involved with violating it. Education of the company policy regarding computer use can not only discourage misconduct, but also can prevent accidental liability issues from employees who didn't realize that an action was harmful or inappropriate.

Monitor Employee Activity

Having a computer usage policy is not enough. The employer must also be diligent in monitoring employee activity, particularly if an individual is suspected of misconduct. Employers should consider implementing a filtering system in their computer network that blocks harmful or inappropriate Web sites based on key words identified by the company.

Let employees know about the filtering system and that the company will be periodically monitoring their computer activities. This will act as an added deterrent for inappropriate behavior or abuse.

For more information on this topic or for assistance in creating an appropriate Employee Computer Use policy, contact The Jacobs Company, Inc. today.