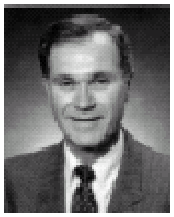
# Business Use of the Internet Usage by Your Employees: Pitfalls and Policies

by Charles H. Melville



*Do you have a group of employees using PCs? Are employees using the Internet for business purposes?*

If you said "Yes" to either or both of these questions, you may suddenly find yourself between the proverbial "rock and a hard place"!

The proliferation of personal computers in the workplace and the increasing use of the Internet for business purposes poses a troubling dilemma and requires drawing a difficult line to guard against liability on a wide range of legal issues including defamation and copyright infringement, protection of your own intellectual property and trade secret information, and the privacy rights of your employees. While drawing that line is difficult and depends on the specifics of your situation, the risk of not drawing the line is even greater.

The spectrum of employee use ranges from a few employees surfing the Net for research purposes, to a full blown on-line marketing program and your own Web site.

No matter what your involvement, we think the most reasonable approach, and the one we recommend, is a formal, written company policy to guide employee usage of the Net. By adopting such a policy, you can minimize your liability exposure based upon employee actions in Cyberspace, protect your own intellectual property, and include reasonable safeguards against claims for invasion of employees' privacy.

### *Checklist for an Internet Usage Policy*

Since individual situations vary so widely, it is impossible to develop a really satisfactory "generic" policy. Therefore, what follows is essentially a checklist of items you should consider in developing a suitable policy.

As with any policy with company-wide impact, you should involve an appropriate range of people, including a variety of affected departments or functions and a variety of levels of function. If you have them, human resources, computer technology, and legal departments should also be involved. Be sure to include both managers and employees actually using the Net.

In addition, although it probably goes without saying, the more employees with access the greater your potential exposure to liability. Therefore, it is generally wise to limit the number of employees with access to Cyberspace to those with a legitimate and business related need for such access.

1. *Prohibit or limit personal use of the Internet via the company network.* Employees should clearly understand that company Internet use is for business purposes only.

2. *Limit participation in online discussion groups to employees who need to do so for business reasons.* This will limit your potential exposure of claims of defamation.

3. *Limit the downloading of information from the Internet.* This will limit your potential exposure to claims of piracy of intellectual property or copyright infringement and, in some cases, sexual harassment (e.g., electronic "pinups" of sexually offensive material). It will also minimize the chances of downloading a computer virus.
4. *Instruct employees to protect the confidentiality of company information.* This should be an extension of

your normal company policy on protecting intellectual property. Remind employees that information sent over the Internet is accessible worldwide. Limit employee access to particularly sensitive company information. Establish a password or security code system, forbid employees to share passwords with unauthorized persons, and consider changing passwords on a regular basis.

5. *Develop or acquire an appropriate training program, and require employees who will have Internet access to attend.* Topics covered should include confidentiality and security issues, intellectual property rights, and review of the Internet usage policy. You may also want to provide "how-to" tips and a primer on Internet etiquette.

6. *If you intend to monitor employee e-mail or other online activities, be sure your monitoring policy complies with state and federal privacy laws.* You may want to specify the purposes for which monitoring may be done, as well as under what circumstances and how it will be done. Also, any monitoring
policy should be communicated to employees in writing before it is implemented. This serves to dispel any expectations of privacy that employees may have with respect to their Internet use.

7. *Avoid "legalese."* Remember that this is a policy which will be used by and must be understood by a wide range of employees.

*8. Include a statement of consequences of violating the company's Internet policies.* Expressly state how violations of the policy will be handled, and identify in detail the range of sanctions, which are to be imposed.

*9. Insist on uniform and consistent enforcement by all management personnel.*

*10. Seek the advice of legal counsel.* If an attorney is not involved in drafting the policy, be sure that legal counsel reviews the policy before it is finalized.

*11. Include the policy in your employee handbook, if you have one.*

*12. Maintain a dated signature log.* All employees should sign an acknowledgment that they have read and understand the policy.