



## Companies must spell out employee e-mail policies

Warren E. Agin  
[Swiggart & Agin, LLC](#)  
Boston, Massachusetts

[WEA@SwiggartAgin.com](mailto:WEA@SwiggartAgin.com)

Your general counsel enters your office with a worried look on her face. Last week you fired an employee for sexually harassing another employee using e-mail. Now the employee is suing the company for violating his right to privacy by accessing his office computer to read his outgoing e-mail messages.

But that's not the worst news. Someone in your marketing department posted a newsgroup article defaming your competitor's product and you were just served with a complaint seeking substantial damages.

Companies already have faced these and similar problems because they failed to recognize the dangers inherent in e-mail and failed to create and communicate clear corporate policies governing e-mail use.

E-mail messages and newsgroup postings share many characteristics with written correspondence. They create a semi-permanent record of the communication which can be saved, forwarded, printed or copied. But because e-mail records are electronic, rather than written on paper, employees often treat e-mail communications like oral conversations, saying things they would never state in a letter or memorandum. This informality creates several dangers.

First, employees might use e-mail for illegal or improper purposes, such as harassing other employees, conducting criminal activities, or in connection with their own business.

Because they perceive e-mail as informal, employees may not realize that a semi-permanent record of the communication exists and will fail to exercise appropriate levels of discretion. Employees may also fail to realize that the return email address will identify the e-mail message as coming from their employer. As a result, the outside world may view an e-mail message or a newsgroup posting as an official corporate communication, when the employee is simply expressing his personal opinion or conducting personal business.

To complicate the matter, in some states employees have rights of privacy in their workspace. Corporations have incurred liability by firing an employee based on evidence obtained from searching a desk or work locker. Employees fired or disciplined for misuse of e-mail have already

sued their employers for violating their right of privacy by accessing their desktop computer and viewing e-mail messages, although, to date, such suits have been unsuccessful.

Second, because employees perceive e-mail as informal, they may use poor judgment in drafting e-mail messages. Employees carelessly treat e-mail messages as conversations, including in them defamatory material, copyrighted material, opinions contrary to corporate policy, messages against corporate interests, or simply poorly chosen content with an inflammatory tone.

Executives sometimes are too honest when using e-mail to discuss sensitive issues, creating dangerous documents which later can be used against the company. E-mail messages should be prepared as carefully as a letter or memorandum, not treated as informal communications.

Third, e-mail messages are not ephemeral. They are stored and retained, sometimes in locations beyond management's control. E-mail messages may remain in storage even when "deleted" on the desktop computer. The recipient of the email message can easily preserve and store the email message, make copies, forward the e-mail message, or even misdirect the e-mail message. Service providers sometimes backup e-mail messages.

In the event of a lawsuit, retained e-mail can be discovered from the company, or subpoenaed from third-parties and used as evidence. Further, messages sent to discussion groups will be read by a wide audience probably including competitors and the press. In other words, you never know how widely an external e-mail message will circulate or how long it will remain in existence.

Creating, communicating, and implementing a clear policy governing e-mail use will help avoid these problems. Companies should include an email policy in their employee handbooks and educate employees about the dangers inherent in email use. To reinforce the message periodically, companies should disseminate copies of the policy to all employees at least annually.

The e-mail policy should clearly define the extent of employees' privacy expectations when it comes to communications via company equipment. The policy should also describe the conditions and procedures under which the company can access employees' e-mail messages. Most policies

inform employees that the company provides e-mail for business purposes, the system is the property of the company and the company may access and disclose the contents of e-mail messages for any business purpose without prior notice to the employee. The policy should also regulate the use of cryptography in connection with email messages. Of course, some companies may want to voluntarily provide greater privacy rights to employees after careful consideration of the risks and benefits involved.

A carefully drafted e-mail policy will also define the company's backup and retention policies. These policies will ensure dig e-mail messages can be deleted in the ordinary course of business without, in the event of litigation, creating allegations of destruction of evidence. A backup and retention policy will also help teach employees that e-mail messages can create semi-permanent records and should be carefully drafted. The corporation should make an effort to understand the backup and retention policies of service providers and affiliates to ensure that its carefully planned retention policy is not undermined by a third party's storage of the e-mail messages. Finally, the company must create and maintain a process to implement the e-mail retention and storage policy.

To maximize the effect of the e-mail policy, the company must commit to educating its employees regarding the proper use of e-mail, and the risks inherent in e-mail use. The policy and educational program should establish guidelines regarding personal use of the e-mail system and provide guidance as to the proper use of e-mail. For example, warn employees not to use the e-mail system for gossip, sexually explicit messages and the like.

E-mail provides a powerful business tool that will eventually be used universally. Companies will have to provide e-mail access to all office employees, just as they provide access to a telephone today. With time, customs and mores for e-mail use will develop, but until they do, companies should protect themselves by using a carefully thought-out e-mail usage policy and educate employees in the proper use of e-mail and the Internet

*Copyright Mass High Tech Communications, Inc., Nov. 18, 1996. Reprinted with permission. All rights reserved.*