Internet and E-mail Acceptable Use Policies (AUP)

By

Michael R. Arkfeld

What action should be taken if someone in your firm accidentally types in an incorrect Internet address and a sexually offensive site is displayed on the screen? What should happen if the site is left on the screen for others in your firm to view? Or what should happen if a disgruntled employee broadcasts by e-mail confidential salary or discipline information to all members of the firm? Do you have a policy if an employee forwards by e-mail a confidential client matter to the wrong party? What should happen if one of your employees leaves a laptop unattended while out of the office and the laptop contains confidential client matters?

With the tremendous increase in technology, law firms have to mandate acceptable use policies (AUP) for e-mail, web access, and other technology applications. The reason firms have to implement AUPs is that they must be concerned about their liability, professional responsibility and productivity. These concerns arise because of defamatory statements, copyright/trademark/trade secret exposure, sexually explicit materials, exposure of office confidential information (salaries, discipline, reviews), employment issues, work productivity, and attorney-client materials, to name a few.

There are several approaches a firm can take toward the use of employee web access and e-mail usage. Some firms prohibit all personal use of the Internet and firm e-mail for personal use. Others realizing that the Internet and e-mail are similar to the use of a telephone request the employees to use reasonableness in using the Internet and firm e-mail addresses. While others impose no limitation on the use of the Internet or a firm's e-mail system.

Whatever approach is used it is necessary to educate employees as to the your firm's legal, ethical and technical policies involved with e-mail, Internet usage and other technologies.

Some considerations:

- Specify the acceptable uses for Internet and e-mail business purposes and personal uses.
- Compare the Internet and e-mail to the phone or fax machine and set out specific penalties for violation of the acceptable uses.
- There should be a written acknowledgement by of what are acceptable uses.
- Implement a training program that updates and monitors the usage of the Internet, e-mail and other technology applications.
- AUPs should be set forth regarding home and remote use of computers, backups, virus checking, use of illegal software, deleting law firm files, encryption, e-mail disclaimers, ownership of digital rolodex files, and working with archived legal materials.

- AUPs should apply to all electronic devices and communications, including individual computers, handheld PCs, PDAs, fax machines, pagers, telephone, and voice mail systems.
- Broad based policies should be in place to explain what is appropriate and inappropriate regarding web surfing - sexually explicit material, hate web sites, racist, or other hostile materials.
- Have specific penalties for violating policy.
- Some law firms, corporations, and other organizations are beginning to implement Internet filtering services to block access to countless web sites. Companies are worried about pornography, hate materials, shopping, music downloading, and other sites that distract employees from their jobs. Things to look for when hiring a web filtering service: cost – usually $10 per terminal per year; references – how long have they been in service, etc.; network support; reports available; scalability; and maintenance requirements.

Some e-mail use policies to consider:

- Mandate all highly sensitive or secretive e-mail be sent by a digital courier or by using encryption software;
- Tell employees messaging will be monitored;
- Place confidentiality notices on all e-mail to assist in protecting the attorney client privileges.
- Forbid message forwarding without the permission of sender;
- Forbid inappropriate material from being sent;
- Provide messaging training;
- Create an atmosphere where employees report unauthorized use of e-mail;
- Make sure everyone knows the e-mail address for the firm;
- Set up a system to hard copy e-mail if you need a permanent record;
- Does the firm offer the option of sending and receiving documents by e-mail to save postage and faxing?
- Should the firm keep a log of e-mail?
- Clients now are calling and asking why you haven't responded to an e-mail message sent a few hours before. Unfortunately, same day responds are becoming unacceptable. Consider automatic reply systems that will e-mail back to all incoming e-mail that you will be gone for a few hours, etc.
- Consider Echomail (www.echomail.com): Eudora (www.eudora.com) or Microsoft Outlook (www.microsoft.com).
- To ensure that clients get and read e-mail and to make sure it remained confidential consider using secure document delivery services that offer various levels of security, features and pricing. Check out: www.certifiedmail.com, www.zixmail.com, www.e-parcel.com, www.sharedoc.com, and www.ziplip.com. UPS offers two secure e-mail services – UPS Online Dossier and UPS Online
- Courier (www.exchange.ups.com). These provide anonymity in the sending and reception of documents.
- E-mail can be altered and signatures changed – check with the alleged sender if there is any question;
- E-mails can be discovered and used in litigation. Assume everyone will be reading your e-mail.
- Passwords do not protect e-mails from being read;
- Assume that e-mail will never be destroyed and that there will always be a copy on someone's server or backup system;
- Remember that an employer generally reserves the right to review and disclose all e-mails messages sent over their system. Do not use e-mail when interpersonal communication is required.

The new technology tools offer a great opportunity for enhanced efficiency in the practice of law. However, with these new technology tools there are circumstances that could lead to possible liability exposure of your firm. With the proper use of AUPs and training many of these risks can be minimized or avoided.

Web Sites:

Model Acceptable Use Policy: Go to www.google.com and type in "model acceptable use policy" for various sites discussing and displaying model use policies. Internet Filtering companies that prevent access to certain Internet sites: SurfWatch (http://www.surfwatch.com), Netnanny (www.netnanny.com), Cyberpatrol (www.cyberpatrol.com), and N2H2 (www.n2h2.com).