Acceptable Use Policy (AUP)

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 and professional responsibility. These concerns arise because of defamatory statements, copyright/trademark/trade secret exposure, sexually explicit materials, exposure of office confidential information (salaries, discipline, reviews), product liability claims, employment issues, work productivity, and attorney-client materials, to name a few.

Some firms prohibit all personal use of the Internet, some request reasonableness, others have no limitation. Some employers argue having AUPs prevents employees from downloading objectionable material, while others argue that it increases productivity. In an age when productivity has gone up dramatically, it may be pound foolish to become too big of a big brother to your employees.

However, it is necessary to educate employees as to the legal, ethical and technical issues involved with e-mail and Internet access.

Some considerations:

- Specify the acceptable uses for business purposes and personal uses.
- Compare it to the phone or fax machine and set out specific penalties for violation of the acceptable uses.
- There should be a formal acknowledge of what are acceptable uses and implementation of a training program with updates and monitoring.
- AUPs should be set forth regarding home and remote use of computers, backups, virus checking, use of illegal software, deleting law firm files, encryption, disclaimers, ownership of digital rolodex files, and working and archived legal materials.
- AUPs should apply to all electronic devices and communications, including individual computers, handheld pcs, PDAs, fax, pagers, telephone, and voice mail systems.

- Broad based policies should be in place to explain what is appropriate and inappropriate web surfing - sexually explicit material, hate web sites, racist, or other hostile

materials.
- Have specific penalties for violating policy.

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;
- References - how long have they been in service, etc.;
- Network support;
- Reports available;
- Scalability;
- Maintenance requirements.