Why You Need An Employee Policy For Electronic Information

James W. Martin
is a probate, real estate, and corporate lawyer in St. Petersburg, Florida, who has written frequently for ***The Practical Lawyer,*** West Publishing, and ***The Florida Bar Journal and News,*** and has more information on his Web site, www.jamesmartinpa.com. The author can be reached at jim@jamesmartinpa.com.

James W. Martin

The answer is easy: To protect client confidences and stay in business.

THE ATTORNEY-CLIENT PRIVILEGE is easily lost. Disclosure to someone other than the client is all it takes. An overheard conversation. A letter discarded in the trash. That's how it used to happen. Before electronics. Now we have email, blogs, Facebook, LinkedIn, and Twitter. A client's entire file can be disclosed to hundreds of people at the click of a mouse. Do we need an electronic information policy for law office employees? You bet we do. And who should write it? You should. It's your policy.

So, what should the office policy say? This article provides sample wording to get you started. It's not exhaustive. It's not tied to a specific state. It's not aimed at big firms, small firms, or solos. It's just wording to get you started thinking about, and writing, your own electronic information policy for employees. Who knows? You might like the wording enough to use it as is. Here we go.

***

A good place to start would be to acknowledge the attorney-client privilege, like this:

Attorney-Client Privilege. Communication with our clients is confidential and privileged from disclosure, whether or not it is in-person

or by phone, email, U.S. Mail, or otherwise. Even our client's names can be confidential. So strong is this privilege that the courts recognize and protect it. However, the privilege can be lost if the confidential information is disclosed to someone else.

Next, the policy should involve the employees in protecting the privilege, such as this:
Confidentiality and Security. All employees must maintain the confidentiality of client information, as well as office password and access security, at all times. In general, this means locking doors and filing cabinets, turning off computers and copy machines, memorizing passwords, keeping office and client documents out of view of others, and not discussing office or client matters in the presence of others.

Now that the basics are out of the way, the policy can make a general statement about office technology and define that term:
Office Technology. Technology helps us provide legal services efficiently, but we must use it wisely and protect the confidentiality of client information while using it. Office technology includes everything from computers, copiers, and scanners to the Internet, email, and blogs. It includes existing as well as future technology.

This would be a good place to state any restrictions on the use of office technology for personal matters:
Personal Use of Office Technology. Office technology is for use in performing work for this law office and its clients. Please do not use office technology for your personal use at any time. Personal matters should not be accessed or stored on office technology and will be deleted.

Are your employees allowed to bring their personal technology to the office for personal use? Can they bring a laptop or cell phone to keep up with their personal email? You must choose from a continuum of possible policies: from no personal use allowed to some personal use allowed to all personal use allowed. Let's start with no personal use allowed. Employees are in the office to work on their employer's business. They should not work on their personal affairs at the office. Therefore, employees should not use office technology for personal use. This is easy to state:
Personal Use of Personal Technology. Your time in the office should be spent on office and client matters, not on personal matters. Therefore, email, Internet, and other technology should not be used for personal matters at the office or during office hours.

But this is not easy to enforce. Email is ubiquitous. Allowing employees to check their email, at least during lunch breaks, might be a fair compromise. The policy might be revised to read as follows:
Personal Use of Personal Technology. Your time in the office needs to be spent on office and client matters, not on personal matters. Therefore, email, Internet, and other technology should not be used for personal matters at the office or during office hours. However, employees may bring their own laptop computers and cell phones to work to check personal email during lunch and other breaks. Office and client matters may not be accessed or stored on an employee's own personal computer or cell phone at any time.

The other end of the continuum would allow full and free use of personal technology in the office, and it would even allow use of office technology for personal matters, so the policy might be further revised to read as follows:
Personal Use of Technology. Employees may use computers, Internet, and other office technology to check personal email during lunch and other breaks. Employees' personal matters may not be stored on office computers and other office technology. Employees are encouraged to bring their own personal laptop computers and cell phones to work for this purpose. However, personal matters must remain separate from office and client matters at all times. Office and client matters may not be accessed or stored on an employee's own personal computer or cell phone at any time.

Surfing the Internet is as ubiquitous as email so it deserves its own mention:

Internet Use. Accessing the Internet at the office or during office hours, other than for office or client matters, is not allowed, except during lunch and other breaks. The above office policies on use of personal and office technology must be strictly complied with.

Social networking has become so prevalent that a policy should be directed toward it:

Blogs and Social Networks. The use of blogs and social networks, such as Facebook, LinkedIn, and Twitter, have become accepted means of business and professional communication and marketing. Our office recognizes and supports this technology to the extent that it complies with this policy manual and the rules of professional ethics and conduct of our lawyers. We recognize, however, that the informality of these networks might tend to reduce the high standard that more formal legal communications usually engender. Therefore, we provide training to all employees in the use of blogs and social networks before employees are allowed to use them in the office or with respect to the office. In no case should a blog or social network be given any client name or client information. Employees should not use blogs or social networks in any manner that would disclose office or client information or adversely affect this office or a client.

The policy should include a provision regarding viruses and other harmful matters, like this one:

Computer Viruses. Computer viruses are a constant threat. An antivirus program is installed on each office computer. In addition, our office has an assigned person in charge of information technology (IT). Each employee needs to assist the IT person and the antivirus software by following a few simple rules:

1. Update the antivirus definitions when starting your computer daily.

2. Do not open or click on an email attachment from an unknown sender.

3. Check for a virus on all other email attachments (copy the attachment to the hard drive and right click to run the antivirus program).

4. Do not install a program, run a CD, or download files from the Internet without approval of the person in charge of IT.

Now let's move to specific technology, starting with hardware. Probably every employee in a law office uses a computer so here is a simple policy for that:

Computers. Each employee is responsible for the safety and security of the electronic information on his or her office computer and for compliance with our procedures for use of computers in the law office. The person in charge of IT will assist each employee in meeting this responsibility.

The other major office hardware read, print, and send electronic information:

Print, Copy, Scan, & Fax Technology. Our printers, copiers, scanners, and fax machines allow us to create and send electronic information at the click of a button, sometimes without even accessing a computer. Every employee needs to be vigilant in the use of this equipment to avoid inadvertently sending office or client information to an unintended party. Every employee needs to comply with our procedures for use of this equipment.

Today we have telecommuting employees who work from home. As we write office policy, we need to keep in mind that everything doesn't happen in the office. Some office things now happen in the employees' homes. Let's write a short policy about that:

Telecommuting and Other Work Out of the Office. When you work on office or client matters from home, at the courthouse, in an airport, or elsewhere, it is especially important that the above policies be followed at all times. Allowing your computer screen to be viewed by someone else could result in loss of the attorney-client privilege. A public computer should not be used to access the office computer system. Using a wireless Internet connection at another lawyer's office, a coffee shop, or elsewhere might allow others on the network to use snooping programs or devices to capture passwords and other

confidential information. The person in charge of IT can assist employees in minimizing this risk.

Remember that these policies are part of an employee policy manual. Your office might have a separate electronic file policy (see my article, *A Model Electronic File Policy for the Law Office*, which appeared in the April 2007 issue of The Practical Lawyer). It might have separate procedure manuals instructing the use of technology. The employee policy manual may refer to these, as follows:

Electronic File Policy; Technology Procedures. For further information on access, use, and storage of electronic information in our law office, please refer to the current versions of our Electronic File Policy and our Procedures Manuals for the specific office technologies.

***

In conclusion, the electronic information section of your employee policy manual can help you integrate current and future technology into your office in a way that promotes efficiency while respecting the attorney-client privilege.