E-MAIL, INTERNET, AND THE WIRELESS AGE

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

LAWYERS MUTUAL | LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

www.lawyersmutualnc.com

DISCLAIMER: *This document is written for general information only. It presents some considerations that might be helpful in your practice. It is not intended as legal advice or opinion. It is not intended to establish a standard of care for the practice of law. There is no guarantee that following these guidelines will eliminate mistakes. Law offices have different needs and requirements. Individual cases demand individual treatment. Due diligence, reasonableness and discretion are always necessary. Sound risk management is encouraged in all aspects of practice.*

JANUARY 2017

E-mail, Internet, and the Wireless Age

Risk Management Practice Guide of Lawyers Mutual

TABLE OF CONTENTS

Introduction	2
E-mail	3
Internet	12
Wireless	14
Conclusion	15
Ethics Opinions Regarding E-mail, internet, and Wireless	16
Creating 'Strong' Passwords	18
Instructions for Wireless Access Points	19
Checklist for Avoiding Inadvertent Disclosure of Confidential Information	21
Sample Internet and E-mail Use Policy	23
Additional Resources	27

LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

5020 Weston Parkway, Suite 200, Cary, North Carolina 27513

Post Office Box 1929, Cary, North Carolina 27512-1929

919.677.8900 | 800.662.8843 | 919.677.9641 FAX | www.lawyersmutualnc.com

INTRODUCTION

Technology changes at an alarming rate. To keep up with the needs of clients, cell phones and e-mail access are necessary for adequate communication. Trying to practice law without these modern conveniences is a handicap you can ill afford to have. Even though the volume of new technology can be overwhelming, being up-to-date is necessary for the prudent practitioner. Well-organized e-mail, smart internet surfing, cell phones and other portable devices can keep your life organized and balanced.

Mobile devices can lead the unwitting attorney into the dangerous trap of a 24/7 practice. However, constant availability is not necessary in most practices. Immediate response to an e-mail or phone call could lead to answering a question wrongly as not all facts were available when the response was given. Accuracy should always trump speed when providing legal advice; no one will remember you were responding to an e-mail at midnight, they will only remember you provided the wrong advice.

As with any other form of communication, new technologies come with new dangers and confidentiality considerations. Every avenue must be explored to ensure that client data is fully protected. Maintaining client confidences is an essential part of practicing law, and knowing how to navigate the technological minefield is important to making sure they are not accidentally leaked. Ignoring the risks of technology opens up serious ethical considerations for an attorney.

“

As with any other form of communication, new technologies come with new dangers and confidentiality considerations.

E-mail

Taming the Beast

Many of us have overflowing e-mail inboxes with more e-mails than we can count. Some of these are e-mails that we need to respond to at a later time. Others are responses to e-mails that we have sent. Some are correspondence from coworkers or other professionals that may or may not be relevant to work. Before e-mail can be a functional tool in our arsenal, we must organize it efficiently. Your inbox should not be a storage unit; it should be used for new e-mails only.

The first step to making e-mail manageable is to clean out your inbox immediately. Organize the e-mails into three basic groups: urgent and important, urgent but not important, and everything else. File away the urgent but not important and everything else categories to handle later. Tackle the urgent and important e-mails now. After you have completed this step, your inbox should be clean and ready for proper use. Be sure to maintain this functionality by managing your incoming e-mails smartly.

Most, if not all, of us have access to spam filters that can eliminate much of the annoying useless e-mail that makes its way into our inbox. Spam e-mails are automatically forwarded to a "Junk E-mail" folder to be reviewed and deleted. Review your spam before deleting it. It is entirely possible a good e-mail was filtered out, such as a hearing notice from the court, and you do not want to explain to the judge that you missed the court hearing because your spam filter trapped the court's e-mail. He may not be understanding.

Folders are also useful for sorting out your general e-mail. E-mails that require action, bills, etc, can all have their own folders, subfolders and be sorted accordingly to be reviewed when necessary. If an e-mail is related to a client file, be sure that a copy of the e-mail is saved to the client's e-file or printed and put in the hard file. E-mails that you receive on a regular basis, such as listservs, can be directed to go directly into a folder so that they are read leisurely and do not clog up the inbox. Be sure to establish a time frame for reviewing e-mails in folders so they don't become overloaded, and e-mails should be deleted when they are no longer needed.

If you receive e-mails from listservs, online shopping resources as well as clients, consider creating multiple e-mail addresses to sort out your multiple roles. Having multiple e-mail addresses will help you keep your most important e-mails in one account and send other e-mails to different accounts to be dealt with separately. Business correspondence, such as from office supply companies and software vendors, can be directed to an e-mail account used specifically for office management. Another e-mail for listservs and memberships will house your profession-related

PRACTICE TIP

ORGANIZE YOUR INBOX AND EMAILS

Your inbox should not be a storage unit; it should be used for new e-mails only.

Clean out your inbox. Organize the e-mails into three basic groups: urgent and important, urgent but not important, and everything else.

correspondence. If you sign up for trial versions of software or have to sign in to visit a specific website, you will need to create a 'spam' e-mail address to catch the solicitations created from these registrations. All of these separate accounts free up your professional e-mail address to only include correspondence related to cases, alleviating the danger that case correspondence could get lost in a flooded inbox.

To assist with maintaining organized e-mail, and protect the firm regarding discovery issues, an e-mail retention policy is often enacted. To develop a logical retention policy, determine a reasonable time frame for keeping e-mail and proper storage procedures for those that are to be kept. E-mails pertaining to client files should be stored with information regarding that file, whether in a hard file or in an e-file. In essence, a file retention policy should allow for the disposal of unnecessary e-mails but provide adequate time for storage of those that need to be kept so that employees are not constantly visiting the IT department to recover e-mails that have been deleted. For law offices, a common practice is to save more, intelligently. Save e-mail correspondence for a set period of time, but be sure to include entire threads or conversations. Should a "smoking gun" e-mail be included in the saved data, the e-mails leading up to the damaging e-mail could include defense material.

A common issue for attorneys is the unsolicited e-mail. Many e-mail correspondences originate from a firm's website, with a potential client seeking advice. To avoid creating a potential attorney-client relationship, all unsolicited e-mails should be checked in the conflicts system by a non-attorney staff member. A standard website notice should inform a potential client that an attorney will not review their request until they have provided basic conflicts checking information. In the event that this person is adversarial to an existing client, you can see how this protection would be vital. You would not want to disqualify yourself by reading an unsolicited e-mail that contained confidential information. In addition to proper conflicts checking procedures, be sure all correspondence originates from within your jurisdiction to practice. With the infinite range of the internet, unauthorized practice of law is a danger as a potential client looking for information may not know you are not licensed to practice in their area.

"Setting guidelines and response times will train your clients on what to expect and provide you with much needed piece of mind to not spend every moment away from the office checking voice-mail and e-mail.

Once you have your e-mail systematically organized, train your clients on the appropriate expected response time to their e-mail and telephone calls to prevent misunderstandings. Clients may think because e-mails are received instantly, you should reply at the same speed. Setting rules as to what constitutes urgent and emergency situations will help establish response time protocols with clients. Response time rules will also help your clients understand that quicker isn't always better; you will need time to review a situation to advise on the proper course of action to take. Setting guidelines and response times will train your clients on what to expect and provide you with much needed piece of mind to not spend every moment away from the office checking voice-mail and e-mail.

Creating a Professional E-mail

Remember that your e-mail is a professional communication, just as if you had written a letter and

mailed it. Most individuals, however, spend much less time and thought in composing an e-mail as done in other correspondence. Simple rules are applied, such as not to use all caps because this constitutes shouting, but professional courtesy is not always extended.

- **Think polite**. First and foremost, never say anything in an e-mail you would not say face to face. If an e-mail comment is misinterpreted or causes confrontation, end the dialogue as back and forth e-mails rarely resolve the issue. Always assume the best when receiving an e-mail as it is easy for text to be unclear as to actual meaning to one person when it is obvious to another. Avoid confusion in your own e-mails by editing and rewording anything that may be misinterpreted. As business correspondence, e-mails should always project respect. Assign the appropriate salutation and closings, if even just a "Thank you," to a close business associate. Also, emoticons and SMS language are not appropriate for business correspondence.
- **Be concise**. Short and concise sentences will assist in making the e-mail easier to read and comprehend. Remember that some of your readers may be accessing their e-mails on a smartphone; making long e-mails cumbersome to read. Be sure that the subject line is used effectively and specifically state the content of the e-mail. This can assist the recipient in determining the importance of the e-mail as well. Contractions can be used in e-mails without sounding unprofessional, however, abbreviations should be limited to familiar expressions that are easily understood.
- **Formatting issues**. Be aware that formatted information does not always translate from one e-mail service to another. Tables or charts copied and pasted from Word or Excel may be received as unformatted garbage. What you see on your screen when you compose the e-mail and send it will not be what the recipient views. If you need to send a chart, attach it to an e-mail to avoid confusion.
- **Sign it.** A business e-mail can also be a great form of advertising. To make this work to its fullest potential, create a signature with your complete contact information. The most important pieces of an e-mail signature are: full name, title, firm name, telephone number, website and e-mail address. You may also include fax number or other relevant information, such as links to social media accounts. If your firm has a logo you can also include it here, but remember that many e-mail systems block image file downloads for security purposes, so the recipient only receives the image if they choose to download it to replace the empty box they see.

PRACTICE TIP

CREATING PROFESSIONAL EMAILS

- **Think Polite**. Never say anything in an email you wouldn't say to someone's face.
- **Be Concise**. Short, concise sentences will make your emails easier to read.
- **Formatting Issues.** Formatted information does not always translate from one email client to another.
- **Sign It.** Create a business signature - it's a great form of advertising.
- **Attachments.** Attach documents before writing email to help prevent sending emails without attachments. Double-check you have the right attachement.
- **Addressing the email.** Turn off auto-complete to make sure you do not accidentally send to the wrong person.
- **CC and BCC.** Use sparingly. Make it clear why person is copied.

- **Attachments**. Before composing your e-mail, attach any document you need to send to the recipient. Attaching files before completing the e-mail helps prevent sending the e-mail without the attachments enclosed, a potential embarrassment that is commonly done. Double check the name of the attachment to ensure you have attached the appropriate document.
- **Addressing the e-mail**. The last step in composing an e-mail should be addressing it. As with attachments, this is a preventive measure so that you cannot accidentally send an incomplete e-mail. Be sure to address the e-mail appropriately as you may have several similar e-mails in your address book. For most accurate addressing, type in the complete e-mail address and avoid using auto-complete or any user-friendly feature of your e-mail program that could lead you astray.
- "CC and "BCC." Use the "CC" and "BCC" features sparingly. "CC" indicates someone needs to be informed of the transaction or who may need to assist with completing requested activities, and it is courtesy to indicate in the body of the e-mail if you are copying someone to request that they follow up with action so that everyone knows why you are copying them. The "BCC" feature is more dangerous as someone who receives a blind copy can forward it or discuss it, leaving the original recipient offended that they were excluded from knowledge that this person also received a copy of the e-mail. For client matters, use "BCC" on e-mails in the same manner you would on a letter sent through the mail to maintain the same sort of propriety.

Confidentiality Issues

Other than organizing your office and presenting a professional image, e-mail presents a risk for breaching client confidences. One of the most dangerous, and easiest, methods of breaking confidentiality is simply sending an e-mail intended for your client to the wrong party. Another trap for the unwary is metadata, the hidden information lurking in attached documents. Training yourself and your staff to avoid these dangers will go a long way in protecting your firm.

- Misdirection. Misdirected e-mails happen all the time. You start typing an e-mail, a name pops up, and you hit enter and send. Unfortunately, it goes to the wrong person before you realize it. To avoid this simple, yet dangerous mistake, turn off auto-complete. This will force you to type in the full address yourself, or copy and paste from your database. Another danger for misdirection is pulling an old e-mail for an individual from your

PRACTICE TIP

CONFIDENTIALTY ISSUES

E-mail presents a risk for breaching client confidences. One of the most dangerous, and easiest, methods of breaking confidentiality is simply sending an e-mail intended for your client to the wrong party.

Steps you can take to protect yourself:

- Turn off auto-complete to address misdirected emails
- Put your disclaimer at the beginning of the email
- Remove metadata before sending attachments
- Send PDFs as image files so they cannot be edited
- Send encrypted emails

address book, sending an e-mail to an attorney's former firm instead of her current employer.

- **Disclaimers**. Many e-mails include disclaimers at the end regarding receipt of misdirected e-mail. Unfortunately, these disclaimers are essentially useless. Consider them the equivalent of including a disclaimer at the end of a written letter than you mailed. If you addressed the letter to the wrong person, does the disclaimer apply? To make a disclaimer effective, place it at the beginning of the e-mail. Only include in the body of the e-mail information regarding who the intended recipient is and why they are receiving the information. Place confidential information in a separate document and attach it to the e-mail. Make sure the recipient would be fully aware that they are not supposed to view the document before they would have a chance to do so, not afterward. To make disclaimers more effective, only place them in documents where confidential information is actually included.
- **Metadata**. Before you send any attachment via e-mail, be aware that documents contain metadata that needs to be removed. Metadata includes everything there is to be known about the document, including former versions, deleted text, and other information you would not want published. The bad news gets worse, as most of us reuse documents from another case. Metadata remembers that, broadcasting the information from the previous case and sharing it with everyone else. Before you panic, you can remove metadata. Microsoft provides features that remove most metadata, and special software called scrubbers will remove nearly all of it. Ethics opinions may dissuade opposing counsel from using metadata against you, but it will not calm the upset client who wonders why the billed time for editing a document is twice the amount of time shown as "total editing time" in metadata.
- **PDFs and image files**. Sending attachments as PDFs will assist in removing metadata, but PDFs also have some metadata of their own. They do not have all of the unsavory data that other documents have, but the receiver will know the creator, date and time the document was produced. PDFs come in two formats, text PDF and image PDF. A text PDF can be edited by someone with the appropriate software while an image PDF cannot. Saving attachments as image files, such as TIFFs, can also eliminate harmful metadata issues and the danger of someone editing the document. In addition to preventing the distribution of metadata, sending attachments as PDFs or image files can add protection by making them less alterable.
- **Encryption**. Another method for protecting confidential e-mail information is encryption. Encrypted e-mails can only be decoded by someone with the same software, so therefore only the intended recipient would be able to read them. Of course, that would require the recipient to have the encryption software as well. This would be advisable for highly sensitive documents.

In addition to the dangers inherent in e-mail itself, you must be wary of sneaky people who have learned that e-mail is a great medium to defraud a law firm. Many of these e-mail fraud scams originate from international sources and are increasingly professional in their appearance of legitimacy.

E-mail Scams

In addition to the dangers inherent in email itself, you must be wary of sneaky people who have learned that email is a great medium to defraud a law firm. Many of these email fraud scams originate from international sources and are increasingly professional in their appearance of legitimacy.

You may receive an email purporting to be from an out-of-state company attempting to collect on a debt owed by a local business or individual. In another scenario, you receive an email that appears to be from another law firm with an attached form for you to download and approve.

PRACTICE TIP

EMAIL SCAMS

To avoid being the victim of an e-mail scam, take precautions. Useful tips to follow:

1. **PAY ATTENTION TO DETAILS**. Grammatical or spelling errors in the email are red flags.
2. **LOOK AT THE "SENDER" INFORMATION**. Most email services still show you the actual address that the email was sent from.
3. **LOOK AT THE CONTACT INFORMATION CAREFULLY**. if you hover over the link – BUT DO NOT CLICK – a different email or website appears.
4. **INDEPENDENT RESEARCH**. Do not rely solely on the information from the email.
5. **PROTECT YOUR TRUST ACCOUNT**. Do not provide your bank or financial information
6. **CHECKS AND BALANCES**. Review your accounts frequently.
7. **TRAIN EMPLOYEES**. Make sure they know what to look for regarding email scams.

In the first instance, the scammer is attempting to defraud your firm by sending a 'certified' check to deposit with instructions to deduct your generous fee from this amount before wiring the remaining funds to the client. In the second situation, the attachment contains malware – most frequently in the form of ransomware, a malicious type of software that holds your files hostage until you pay a large fee.

To avoid being the victim of an email scam, take precautions by thoroughly investigating any potential client that contacts you only via email. Here are some useful tips to follow:

- **Pay attention to details**. Typically in these situations, there are grammatical or spelling errors in the email. Some of these are intentional to pass through your security measures to prevent your email system from blocking them.
- **Look at the "Sender" information**. Scammers will spoof real accounts, but most email services still show you the actual address that the email was sent from. If something purporting to be from 'jane@xyzlawfirm.com' comes from '123x3d@gmail.com', you should assume this is a scam and handle it as such.
- **Look at the contact information carefully**. Most scammers include contact information for real companies. However, if you hover over the link – place your mouse over it BUT DO NOT CLICK – a different email or website appears.
- **Independent research**. Do not rely solely on the information the email provides you. You are uncertain regarding the validity of an email, look up the company and sender, then use the information obtained from this search to contact them.
- **Protect your trust account**. Do not provide your bank or financial information. This information can be used to withdraw money from your account. Bank tellers sometimes try too hard to please the customer standing in front of them and do not verify identity properly.

- **Checks and balances**. Review your accounts frequently so that you can be aware of theft and take appropriate action quickly.
- **Train employees**. Make sure everyone in the office is aware of what to look for regarding email scams. Too often an employee used to handling a certain type of activity falls victim to a scam.

Wire Fraud

Lawyers Mutual has received multiple reports of North Carolina attorneys who were targeted by scammers attempting to divert seller closing proceeds following real estate transactions.

It appears hackers first became aware of the closing by compromising email accounts of differing parties. Sometimes the attorney account was compromised, sometimes the Seller's account was compromised but the most common scenario was the Realtor's account was being monitored by international criminal organizations. The foreign-based hackers would observe the account, likely for several weeks, and only actively intervene once an understanding of the business practices were obtained and a significant wire was to be produced. In the interim, the unsuspecting Realtor would continue to use the account unaware his or her client and the closing attorney were being set up to be robbed.

We have seen a rise in wire fraud relating to the interception of incoming wires. Here are the best practices to prevent these claims:

- It is our strongest recommendation that all parties in the transaction be notified of proper wiring procedures as early in the closing process as possible, preferably in an engagement letter. This notice should be not be sent with the wiring instructions. Suggested language to include in your engagement letter:

  Pursuant to the N.C. Gen. Stat. §45, ALTA Best Practices, State Bar Rules and in order to protect your funds, all funds in excess of $500 must be received by wire to XYZ Law Office. For this transaction, the only bank account we will be using is our IOLTA Trust Account, described and partially redacted below:

  YYZ Law Office IOLTA Trust Account

  Bank of America

  123 Main Street

  Raleigh, NC 27603

  *Partial ABA # *******72*

  *Partial Account # *******184*

  Before Sending Any Wire, Call Our Office At (919)555-5309 To Verify The Instructions. We Will Not Change Wiring Instructions. If You Receive Wiring Instructions For A Different Bank, Branch Location, Account Name Or Account Number, They Should Be Presumed Fraudulent. Do Not Send Any Funds And Contact Our Office Immediately.

  Failure To Follow This Procedure Endangers Your Funds

Lawyers Mutual has received multiple reports of North Carolina attorneys who were targeted by scammers attempting to divert seller closing proceeds following real estate transactions.

- Have the client sign and return the notice to your office. If it is part of a larger engagement letter, this section should be initialed.
- Wiring instructions should only be sent to the buyer/intended recipient. Allowing wiring instructions to be forwarded through a Realtor or other party allows an additional point of interception, adds to the delay of their receipt, and prevents other security measures.
- The full wiring instructions should be sent in an as secured manner as possible when the recipient is expecting their delivery. Ideally, the client would call your office for the wiring instructions, the client's identity would be verified and they would wait on the open line until the instructions are received via secured email or facsimile.
- Wire receipts should be verified either through calling the bank directly or securely logging into the banking portal. Do not rely upon an email or fax verification of receipt of the wire from your bank. We know of situations in which fraudsters sent 'confirmation of wire' or 'advice of credit' notices with the intent of delaying discovery of the theft. Failing to properly verify receipt could result in a closing attorney disbursing non-existent funds from the trust account –increasing the attorneys' liability and creating ethical problems with the State Bar.
- Take every opportunity to educate the client on the need to confirm wiring instructions before initiating a wire.

PRACTICE TIP

WIRE FRAUD

To avoid being the victim of wire fraud, use these best practices:

1. Send an engagement letter with proper wiring procedures as early in the closing process as possible,
2. Wiring instructions should only be sent to the buyer/intended recipient
3. The full wiring instructions should be sent in a secure manner, and when the recipient is expecting their delivery
4. Wire receipts should be verified either through calling the bank directly or securely logging into the banking portal
5. Educate the client on the need to confirm wiring instructions before initiating a wire.

Other Issues

So that the entire firm presents a professional e-mail image, create an e-mail usage policy for attorneys and staff. Having rules established that list what is acceptable and what is forbidden prevents potentially problematic situations. Establish a full scope of what is included in the policy, such as who, what, when and where. While most employees will avoid pornographic material at the work place, other issues will arise that should be addressed before they become problems. The policy should also include appropriate action taken if the rules are broken so that employees understand the consequences of disobedience.

So that the entire firm presents a professional e-mail image, create an e-mail usage policy for attorneys and staff. Having rules established that list what is acceptable and what is forbidden prevents potentially problematic situations.

- **Personal use**. Many of us have received forwarded jokes or religious e-mails that travel through cyberspace as neverending cycle. These have no place in the office. A recipient can easily be offended, and they simply waste time and take up space. Limiting or prohibiting personal e-mail use is completely within the rights of the firm. Remember, the firm owns the e-mail and has the right to review it without the consent of the employee. Personal e-mails should be handled through a personal e-mail account, which can easily be obtained through a free service such as Yahoo or Gmail. While the firm has the right to limit access to such accounts, it is much better to encourage employees to have personal e-mails go to personal accounts than allow such junk mail to clog up the business inbox.

- **Negativity**. It is also imperative to make attorneys and staff aware that anything they say in an e-mail can and will be used against them, so take great care not to be derogatory in any situation. Also keep in mind that sarcasm is completely lost in cyberspace. Even if the intended recipient knows you and understands the intent, someone else may not. E-mail conveys no emotion and what you say can easily be misconstrued by someone who is not completely familiar with you. An e-mail is a permanent record of a thought, and it can be forwarded around the community at the speed of light. Mistakenly hitting "Reply to All" instead of "Reply to Sender" can cause a tidal wave if a comment has a negative tone. Even if you do not send a negative comment to the wrong person, your e-mail can be forwarded. Any negative e-mail sent by an employee damages the image of the firm. If you do not want to see your comment in the news, do not put it in writing and send it.

- **Home business**. It is very easy for an employee to use a firm's resources to run a home "business," such as selling Avon or refereeing little league sports. These activities can detract from the amount of work completed during business hours and interfere with the ability of others' to do their jobs properly. A firm will need to determine if they will prohibit any use of resources, even during break, lunch or after hours, for such activities. Charity and other such activities must also be addressed.

Internet

In addition to properly handling e-mail, your internet connection itself must be secure to maintain confidentiality. Internet security has three main components: anti-virus, firewall and spyware protection. All three are necessary to ensure that your data is safe from predators.

Anti-virus

Anti-virus software is probably the most familiar and most likely to be installed on your computer. It protects against malicious code hidden in files, often sent via e-mail. Some online e-mail providers, such as Yahoo, automatically scan e-mail for viruses and place a notice on the e-mail if an attachment is viral, or it will block the attachment from coming through altogether. If you do have an attachment you are downloading, your virus scan software should automatically scan it for viruses before allowing you to download it. If not, change software immediately.

Firewall

Firewall protection stops hackers from logging into your computer. Yes, there are actually people out there who would violate your privacy by breaking into your system and stealing your information. Not having firewall protection is the equivalent of having a key to your front door under a doormat that reads "Welcome!" Firewall software can be bundled with anti-virus or purchased separately, but you must have it.

Spyware

Spyware protection is probably the least familiar for most consumers. Spyware protection prevents malicious behind-the-scenes software from websites you visit from being installed on your computer that records your computer's information and reports it back to the evil genius that created the software. It will also scan and remove those annoying cookies that build up in your temporary files and slow your computer down to a crawl. Spyware protection catches the hidden dangers that anti-virus and firewall protection overlook.

Updates

Even if you own all three, you are not simply out of the woods. You must be sure to keep all of your software up to date. Those Windows updates that force you to reboot your computer at the most inopportune times could be the difference between protected and vulnerable. If you own a version of software that is no longer being regularly updated, upgrade immediately. Just because it works doesn't mean it's okay to continue using. Unsupported software can have holes that are unpatched and are an easy entryway for attackers.

IM/Chat

Another method of circumventing protection is instant messenger services. Most of these services allow for the transfer of documents without downloading them outside of the software. This prevents anti-virus software from immediately scanning documents for malicious contents. IM software can be useful for firm interaction, especially for firms with multiple locations, but you should be aware of the dangers if attorneys and staff download documents from outside sources. Weigh the dangers and benefits of IM services and determine if blocking access to them should be part of your firm's policy.

Surfing

Your browser can be one of the most dangerous pieces of software on your computer. Without proper security settings, it is the largest open window for viruses and spyware known to man. Simply shopping around for a legitimate work-related item can have you visiting sites that download tons of harmful items to your system. To protect yourself to the fullest, be sure your "privacy" setting is set to medium or higher. This limits cookies that can be downloaded and used to record your information. You can also configure your security settings so that you are prompted to download any required plugins and any unsigned or not marked safe plugins are immediately disabled. These settings will prevent viruses and spyware from being downloaded into your system while you're trying to view a site. You can also use the settings on a browser or a toolbar to block popups, creating more armor against spyware and further protecting yourself while you surf. Also, be smart about the sites you visit. If it doesn't look quite right, don't go.

Home Computer

Many attorneys may also access the network via their home computer. Even if your home computer is hardwired for internet service, this can be a dangerous venture. Using a compromised home computer to log into the office can bypass firewalls and other security measures, creating a breach. Why is your home computer so dangerous? Children are less scrupulous about the files they download, and a shared computer can be overrun with spyware faster than you can blink. Children are also creative about circumventing protection to get to the files they want. Do not access client files on a computer that a child uses unless you have partitioned the hard drive. While it would be best not to use a shared computer, it is not always possible. Partitioning the hard drive keeps the files you access safe from the files your child accesses, provided you maintain proper password protection protocols so your files aren't accessible if you are on a coffee break.

PRACTICE TIP

Your internet connection itself must be secure to maintain confidentiality. Look into the following internet securities:

- **Anti-virus software**. Potects against malicious code hidden in files, often sent via e-mail.
- **Firewall**. Stops hackers from logging into your computer.
- **Spyware**. Catches the hidden dangers that anti-virus and firewall protection overlook.
- **Updates**. Diligently update your software when prompted. Unsupported software can have holes that are unpatched and are an easy entryway for attackers
- **IM/Chat**. Can be a system vulnerability as prevents anti-virus software from immediately scanning documents for malicious content.
- **Surfing**. Your browser can be one of the most dangerous pieces of software on your computer. Without proper security settings, it is the largest open window for viruses and spyware.
- **Home Computer**. Using a compromised home computer to log into the office can bypass firewalls and other security measures, creating a breach.

Wireless

Because so much time is spent out of the office for various purposes, we all have several devices to make keeping connected easier. Laptops, smartphones, USB flash drives, and blue tooth headsets are just a few of the modern conveniences that we use everyday. They are also easy ways to lose client data when we are not on the top of our game.

Laptops

Many attorneys never leave home without their laptop computers. These wonderful inventions allow us to be productive waiting in the airport or during breaks at a CLE event. They also provide multiple opportunities for loss of data by their very nature. Many of these computers are left behind when travelling, and losing track of your laptop becomes easier the smaller they get. First and foremost, do not let your laptop out of your sight. Secondly, any computer that leaves the office should be password protected, meaning that every time your screensaver activates you have to enter the password to get back to your data. A laptop's memory can hold the equivalent of a small self-storage unit worth of files. With this much at risk, encrypting your data or purchasing a remote wipe program should your laptop become lost does not seem like a bad idea, does it?

Wireless Connections

Other than the danger of accessing the laptop itself, wireless internet connections used when travelling can be easy portals into your computers if proper precautions aren't taken. Even your home wireless connection can be a problem if proper security isn't set up. Simple steps to ensure your home network is safe include making sure your network isn't discoverable and changing your security setting to WPA. Be sure you have the newest technology and enable all possible security features. Make sure all passwords and the SSID are changed from their defaults. Use a firewall for your wireless access point and keep your network software updated.

“ Laptops, smartphones, USB flash drives, and blue tooth headsets are just a few of the modern conveniences that we use everyday. They are also easy ways to lose client data when we are not on the top of our game.

If you are out of the office and must use a public access internet connection, be aware that these connections are not secure. A hacker can easily install keylogging software that records what you type, passwords included, and have access to all of your files. Some hackers even go so far as to create a dummy network mirroring the location you want, hoping you'll log into their system and provide them all of your data freely. If you are in a public hotspot and find two similarly named networks, verify the correct name before logging on. Always use a VPN (virtual private network) to connect to the office's database. VPN's encrypt the connection so that any intercepted data is unreadable.

Smartphones/Tablet computers

Perhaps just as dangerous are the hottest toys on the market, the smartphone and the tablet computer. These mini-computers can hold tons of information, including your entire inbox from your e-mail provider. There are also apps available that allow you to edit documents. Considering that the phone itself fits in your pocket (and the tablet is not much bigger), you can image how easy it is to leave in a cab or in a restaurant. All of the rules for a laptop apply to a smartphone: password protect, encrypt data, and purchase a remote wipe program. Yes, the phone has a GPS locator that will find it, but in that time someone could have downloaded all of your files to another device and posted them on Facebook or Twitter.

USB Flash Drives

USB flash drives are the easiest piece of equipment to lose. Most of the data on USB drives is left unencrypted and ripe for the taking. Unfortunately, there is not a remote wipe function for USB drives. USB devices can be password protected and encrypted. Some devices come with these features built in. If your device does not have encryption software, you can purchase software for it. Obtaining security features for flash drives is definitely critical if you use them as your main source of backup and this tiny piece of equipment contains all of your confidential data. Of course, the optimum solution is to never lose the USB drive, but the world is never perfect.

Bluetooth

Bluetooth technology is another hidden danger. Malicious software can actually be downloaded through your Bluetooth. With the proper equipment, someone can listen in and record your conversation. Turn off the "discoverable" setting and turn your device on only when in use.

Too many Bluetooth users also increase the volume of their voice when using the headset. These loud conversations can easily be overheard by anyone in close proximity. Start using your inside voice for Bluetooth conversations or take off the headset and use the phone the old–fashioned way. You never know who may know someone related to the case and may tell everything they heard!

Conclusion

Modern technology provides many conveniences that make practicing law easier. These technologies help attorneys maintain a balance between work and social life by affording them the ability to be out of the office without fear of being unobtainable when needed. Mobile connectivity is now a part of everyday life that cannot be overlooked or avoided.

These conveniences, however, can also be pitfalls if we do not properly manage them. Ensuring they are protected is an attorney's responsibility. Your information is only as safe as the weakest part of your security system. Installing proper security features and keeping software up-to-date will go a long way to protect client data. Know your device and take appropriate precautions to maintain it. If you are unsure how to properly secure your equipment, contact a professional to help you.

ETHICAL OPINIONS REGARDING E-MAIL, INTERNET AND WIRELESS

- **ABA Opinion 11-459: Duty to Protect the Confidentiality of E-mail Communications with One's Client**

  A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.

- **ABA Opinion 11-460: Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel**

  When an employer's lawyer receives copies of an employee's private communications with counsel, which the employer located in the employee's business e-mail file or on the employee's workplace computer or other device, neither Rule 4.4(b) nor any other Rule requires the employer's lawyer to notify opposing counsel of the receipt of the communications. However, court decisions, civil procedure rules, or other law may impose such a notification duty, which a lawyer may then be subject to discipline for violating. If the law governing potential disclosure is unclear, Rule 1.6(b)(6) allows the employer's lawyer to disclose that the employer has retrieved the employee's attorney-client e-mail communications to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law. If no law can reasonably be read as establishing a notification obligation, however, then the decision whether to give notice must be made by the employer-client, and the employer's lawyer must explain the implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision.

- **ABA Opinion 99-413: Protecting the Confidentiality of Unencrypted E-Mail**

  A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.

- **2002 Formal ethics opinion 5: Retention of E-mail in a Client's File**

  Opinion rules that whether electronic mail should be retained as a part of a client's file is a legal decision to be made by the lawyer.

- **2008 Formal ethics opinion 5: Web-based Management of Client Records**

  Opinion rules that client files may be stored on a website accessible by clients via the internet provided the confidentiality of all client information on the website is protected.

- **2009 Formal ethics opinion 9: Review and Use of Metadata**

  Opinion rules that a lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication and a lawyer who receives an electronic communication from another party or another party's lawyer must refrain from searching for and using confidential information found in the metadata embedded in the document.

- **2011 Formal Ethics Opinion 6: Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property**

  Proposed opinion rules that a law firm may contract with a vendor of software as a service provided the lawyer uses reasonable care to safeguard confidential client information.

- **RPC 215: Modern Communications Technology and the Duty of Confidentiality**

  Opinion rules that when using a cellular or cordless telephone or any other unsecure method of communication, a lawyer must take steps to minimize the risk that confidential information may be disclosed.

- **RPC 252: Receipt of Inadvertently Disclosed Materials from Opposing Party**

  Opinion rules that a lawyer in receipt of materials that appear on their face to be subject to the attorney-client privilege or otherwise confidential, which were inadvertently sent to the lawyer by the opposing party or opposing counsel, should refrain from examining the materials and return them to the sender.

- **2012 Formal Ethics Opinion 7 — Copying Represented Persons on Electronic Communications**

  Opinion provides that consent from the lawyer for a represented person must be obtained before copying that person on electronic communications; however, the consent required by Rule 4.2 may be implied by the facts and circumstances surrounding the communication.

Creating 'Strong' Passwords

Passwords can be the weakest link in a computer security scheme. Strong passwords are important because password-cracking tools continue to improve and the computers used to crack passwords are more powerful. Network passwords that once took weeks to break can now be broken in hours.

Password cracking software uses one of three approaches: intelligent guessing, dictionary attacks, and automation that tries every possible combination of characters. Given enough time, the automated method can crack any password. However, it still can take months to crack a strong password.

For a password to be "strong" or harder to break, it should:

- be at least seven characters long;
- contain at least one character from each of the following four groups:
  - uppercase letters A, B, C, ...;
  - lowercase letters a, b, c, ...;
  - numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9; and
  - symbols (all characters not defined as letters or numerals, including: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
- have at least one symbol character in the second through sixth positions;
- be significantly different from any passwords you have used previously;
- not contain your name or your computer user name;
- not be a common word or name.

Treating passwords as confidential keys to your computer assures you and your staff secure your client's data.

The following are some steps you can take to protect your passwords and keep your data secure:

- Never write down your password, especially on your monitor. Is this not the same as leaving the keys for your car in the ignition? Take a walk around your office and see how many passwords you can find on monitors.

- If you absolutely have to write down some of your passwords to remember them, don't write them out exactly. Write them out so they have to be translated in some way. For example, add or delete a character, transpose letters, or vary them some other consistent way which only you can figure out.

- Don't tell anyone your passwords. Change any compromised password immediately, even if you only suspect it has been compromised.

- Don't use the same password for everything as you could be giving someone full and easy access to your entire system. Try to use different passwords for different programs, especially for your network logon password.

- On Windows 2000 and XP computers, don't have identical passwords for your network logon and administrator account passwords.

- Ideally you should change your network password every 60 to 90 days.

- Be careful about where you save your password on your computer. It is not uncommon for people to have a Word or WordPerfect file with all their passwords in it. This file can be easy to find, especially if it is called password.doc, or if it contains the word "password."

- Be wary of dialog boxes, such as those for remote access and other telephone connections, that present an option to save or remember your password. **Do not select this option.**

Instructions for Wireless Access Points

#1 - CHANGE THE ROUTER PASSWORD

Most APs will challenge you for a password when you attempt to access the configuration interface. Routers of a given make and model are manufactured with a standard or default password. This will be listed in your manual. Not only are these passwords common words such as "admin", they are widely known and can easily be determined from a search of the Web. Hackers will try to access and change an AP's settings to make it easier to connect to. Changing the default password makes it much more difficult for a hacker to access a router's configuration interface.

#2 - DISABLE REMOTE ROUTER ACCESS

To make it easier for IT people to administer a network, many APs have a remote administration or access feature which allows configuration changes to be made from a remote location across the internet. While this is more convenient for IT people, it also allows a hacker access your router across the Internet. Turn off the remote access feature to prevent a hacker from accessing your router across the Internet. Note that turning off remote access also prevents you from making configuration changes to an AP across a wireless connection. For this reason, after making this change you can only make configuration changes to your router from a computer that is connected to it by an Ethernet cable.

#3 - DISABLE SSID BROADCASTING

So that they are easy to locate and connect to, APs broadcast a *service set identifier* or *SSID*. This SSID is the name of your wireless network. The radio signal from your AP will radiate in a sphere 20 to 35 metres or more in diameter. With SSID broadcasting enabled, the name of your network is broadcast to all that can receive a signal from your AP. Wireless-enabled laptops and PCs can scan their surroundings for SSID's, and will display a list of all network SSIDs they can pick up signals for. To stop your AP from advertising its presence, you need to disable SSID broadcasting. This effectively hides your AP from snoopers looking for wireless networks.

#4 CHANGE THE DEFAULT SSID

Even if you turn SSID broadcasting off, a hacker can easily connect to an AP if they know the appropriate SSID. Specific makes and models of APs are configured with a default SSID. These are common terms such as "network", and are widely known or easily determined. Thus, even with SSID broadcasting turned off, a hacker could find an AP by trying to connect with a default SSID. For this reason, you want to change the default SSID on your AP to something that only you will know. Change it to something that is not obviously connected to you (i.e. don't use your name, street name etc.) or any common word. Ideally you should use a combination of letters and numbers. You will have to give the same SSID to all the wireless devices on your network.

#5- TURN ON THE AP FIREWALL

Most wireless APs also have their own firewall, which in most cases, is turned on by default. If your AP has a firewall, it should be turned on. Review and turn on any firewall settings that will offer better protection for your network. The block anonymous Internet requests setting is on most AP firewalls, and should be enabled. For maximum security you should also run a software firewall on the computers on your network.

#6 - ENABLE DATA ENCRYPTION

Passwords and data transmitted by wireless devices can be intercepted and read by anyone who picks the wireless signals up, especially at the point where wireless devices are initially connecting to one another. To prevent this from happening, you need to enable encryption features. All APs have encryption capabilities.
Wired Equivalent Privacy (WEP) is the oldest form of encryption, and is on most APs in use today. It is not very secure, but is better than nothing. WPA (Wi-Fi Protected Access) is a newer form of encryption and it offers much more protection than WEP. The newest wireless devices will have WPA2, which offers the best security (some WPA devices can be upgraded to WPA2). Unfortunately, WEP and WPA aren't compatible with each other. Use WPA or WPA2 only if all your devices have it, otherwise you will have to use WEP.

After you enable WEP or WPA, you will see further configuration settings in your interface. Check your router manual for more information on these settings and configure them as appropriate.

#7 - ENABLE MAC FILTERING

Every network device has a unique identifying number assigned to it called the Media Access Control or MAC address. MAC addresses give devices a unique identity, and are used by network operating systems to move data from one device to another. Enabling MAC filtering in your AP improves security by letting you specify the MAC addresses of wireless and network devices that your AP can communicate with. After making this change wireless devices with unrecognized MAC addresses will be unable to connect to your AP. You will have to add the MAC address of each device on your network to the list on your AP, and then enable MAC filtering. MAC addresses are usually printed on a sticker that is attached to a wireless network card, or on the bottom of a wireless-enabled laptop.

A Checklist for Avoiding Inadvertent Disclosure of Confidential Information and Privileged Communications

The following checklist for avoiding inadvertent disclosure of information is from an article by Willis S. Baughman in the Lawyers Mutual Insurance Company of California's Spring 2008 Bulletin. It contains guidance for both lawyers sending and receiving documents. We have modified the checklist to show North Carolina authority when applicable.

TIPS FOR "SENDING" LAWYERS

- On all outgoing documents include an appropriate legend indicating:
    - Privileged & Confidential
    - Attorney-Client Communication
    - Attorney Work Product
- Avoid using "Reply All" feature in replying to e-mail.
- Avoid using "Speed Dial" feature for facsimile transmissions – instead manually punch in numbers.
- Be cautious when disconnecting from conference calls.
- With respect to all modes of communication check carefully before sending!
- Sad but true: If you don't know and trust your adversary, guard your files!
- Once it is discovered that privileged or confidential information has been inadvertently sent, immediately contact the receiving lawyer. Consider as guidance proposed Federal Rule of Evidence Sec. 502 that provides:
    - Inadvertent disclosure of protected communication or information is not a waiver if:
        - The sender took reasonable steps to prevent disclosure; and
        - The sender employed reasonably prompt measures to retrieve the mistakenly disclosed communications or information.
- Special tips for sending electronic documents:
    - Eliminate metadata with scrubbing programs.
    - Train personnel to use programs that clean and seal documents before sending them to a third person.
    - Establish policies and procedures to apply to all outgoing documents.
    - Avoid sending the electronic document in the first place.
    - Save and transmit documents in non-electronic formats, such as:
        - Hard copy;
        - Create an image; and
        - Print and fax.

TIPS FOR "RECEIVING" LAWYERS

- The moment it becomes reasonably clear that the material was inadvertently sent and not intended for you:
    - Review the material only to the extent necessary to ascertain if it is in fact privileged or confidential.
    - The moment it becomes reasonably clear the material is privileged or confidential follow the guidance in North Carolina State Bar ethics opinion RPC 252 (1997) that provides:
        - A lawyer in receipt of materials that appear on their face to be subject to the attorney-client privilege or otherwise confidential, which were inadvertently sent to the lawyer by the opposing party or opposing counsel, should:
            - refrain from examining the materials; and
            - return them to the sender.
- Work with the sending lawyer to resolve the situation through mutual agreement.
- In situations where mutual agreement is not feasible or possible seek judicial guidance:
    - Consider using judicial intervention;
    - Consider protective orders where necessary.
- Act fairly and reasonably:
    - Take steps that protect not only your client's interest, but also the legitimate interests of the opposing lawyer and his client
    - Take steps that are in accord with the core value and dignity of:
        - The legal profession;
        - The attorney-client relationship;
        - The judiciary;
        - The administration of justice.

Sample Internet and E-mail Use Policy

By David J. Bilinsky [1]

FOREWORD

Use of e-mail and the Internet can result in a huge productivity increase for a law practice. Through e-mail, lawyers and their staff can save time by avoiding telephone tag and voice mail jail and can save money by avoiding long-distance telephone calls and the transmission of documents by costly methods such as faxes or long-distance couriers. Moreover, use of e-mail says to clients that your firm knows how to take advantage of the latest communication methods for everyone's benefit.

E-mail can, however, also expose a law firm to embarrassment, unwanted media exposure and litigation. Increasingly lawyers are becoming adept at discovery of electronic evidence such as e-mail, including e-mail the User thought had been deleted, but in fact has remained in data back-ups or on unerased hard drives.

It is prudent for a law firm to take a reasoned policy approach to the Internet that balances the innovative and productive use of Internet resources against inappropriate use.

This policy is intended as a sample, not a model. It does not and cannot purport to be the best of all possible policies, for the simple reason that any precedent must be modified to meet the needs of your firm, your clientele and your practice. In particular, this Internet and E-mail Use Policy should also be considered in light of federal or provincial protection of privacy legislation that may at some point extend to law firms.

This document will be amended from time to time. The firm must take steps to introduce the policy initially to all staff, take steps in order that all new staff are made aware of the policy, and lastly that all changes are communicated to all members of the firm.

I. POLICY SCOPE

This "Internet and Electronic Mail Use Policy" applies to all Firm employees, partners and associates, guests and third-parties (hereinafter "Users") whose access to or use of Internet and e-mail resources is provided by the Firm or available through equipment owned or leased by the Firm, whether or not that access is during normal working hours and whether such access is from the Firm's premises or elsewhere.

II. POLICY PURPOSE

This Policy is to establish guidelines and minimum requirements governing the acceptable use of the Firm's Internet and electronic mail (Internet and e-mail) resources.

---

[1] *The author gratefully acknowledges the prior work of Jerry Lawson, author of The Complete Internet Handbook for Lawyers, published by the American Bar Association, and Jane M. Savard, Internet, technology and small business lawyer of Seattle, Washington, in their respective sample Internet and E-mail Use policy statements. These statements have served as precedents for this document and portions of which have been incorporated into this document.*

By the Firm establishing and maintaining compliance with this policy, the benefits of these communication tools can be realized while the risks and costs are mitigated. The objectives of this Policy are to ensure that:

- use of the Firm's e-mail and Internet resources are related to, or for the benefit of, **[name of law firm] (hereinafter "the Firm")**;
- users understand that e-mail messages and documents may be subject to the same laws, regulations, policies and other requirements as information communicated in other written forms and formats;
- disruptions to the Firm's activities from inappropriate use of the Firm's e-mail and Internet services are avoided; and
- users are provided guidelines describing their personal responsibilities regarding confidentiality, privacy and acceptable use of the Firm's Internet and e-mail as defined by this Policy.

III. PRINCIPLES OF ACCEPTABLE USE

As with any resource provided by the Firm, Internet and e-mail resources should be dedicated to legitimate Firm business activities and governed by rules of conduct similar to those applicable to the use of other information technology resources. The use of Internet and e-mail resources imposes certain responsibilities and obligations on all Users and is subject to the Firm's policies and procedures and all provincial and federal laws.

Acceptable use must be legal and ethical. Acceptable use demonstrates respect for intellectual property, ownership of information, network system security mechanisms, and individuals' rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance. Furthermore, the nature of e-mail raises expectations for a timely response — all Users are urged to read and respond to all e-mail in a prompt and courteous manner.

All Internet and e-mail use shall:

- respect and uphold the law, including provincial and federal laws and regulations and the laws of other jurisdictions;
- comply with the Firm's stated policies, procedures and standards;
- be courteous and follow accepted standards of etiquette;
- protect others' privacy and confidentiality;
- reflect responsible use of e-mail and Internet resources;
- use information technology resources efficiently and productively; and
- contain a clause that claims lawyer confidentiality over the contents of any communication.

IV. ACCEPTABLE AND UNACCEPTABLE ACTIVITIES

Acceptable Internet and e-mail activities are those that conform to the purpose, goals, and mission of the Firm and to each

User's job duties and/or responsibilities. The following list, although not exhaustive, provides examples of *unacceptable* uses:

- engaging in the unauthorized practice of law in other jurisdictions;
- engaging in any illegal activity or using the Firm's resources for any illegal purpose;
- knowingly disseminating harassing, abusive, malicious, sexually explicit, threatening or illegal information, including jokes or cartoons;
- using the Firm's resources for purposes unrelated to the Firm's business activities, such as personal commercial use, advertisements, solicitations or promotions;
- using the Firm's resources to send messages expressing controversial, potentially offensive and/or defamatory comments of individuals, bodies corporate or groups including, but not limited to, religion, politics and social policies;
- downloading or using the material, software or other intellectual property of others in violation of software licenses, copyright and trademark laws;
- disclosing any passwords or security means and methods adopted by the Firm;
- downloading or using any software not approved for use by the Firm;

Users may use the Firm's Internet and e-mail resources for incidental and occasional personal use, provided that such use is reasonable in duration, does not result in increased costs to the Firm and complies with this Policy, in particular Section V (Other Use).

Furthermore, Users must recognize that electronic correspondence is not inherently private, that messages could be misdirected and that the Firm takes no responsibility resulting from the disclosure of private communications occurring over the Firm's resources. Furthermore, the Firm retains the right to monitor any and all electronic communications and use of the Internet to ensure the integrity of the system and compliance with this Policy. Users are reminded that ALL documents, including electronic copies, may be subject to a court order and, as such, disclosure may apply to a User's personal documents as well as any work-related documents.

Users are urged to keep in mind that, if they do not wish their mother to read about it in the media (e.g., *Province* or *Vancouver Sun*), they should not put it into an e-mail message.

Furthermore, use of Internet and e-mail resources may be subject to limitations as determined from time to time by the Firm's supervising authority. Users are advised to remove themselves from e-mail and Internet lists not dealing with work-related topics.

V. OTHER USE

All use of the Firm's Internet and e-mail resources for commercial purposes unrelated to the Firm or for non-commercial, charitable or not-for-profit uses must first be approved in writing. Any such use must comply with this Policy.

VI. PRIVACY CONSIDERATIONS

Files in Users' accounts and data on the network are regarded as personal: that is, the Firm does not routinely monitor this information. However, the Firm reserves the right to view or scan any file, e-mail or software stored on the Firm's systems or transmitted over the Firm's networks and may do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses or unauthorized software), or to audit the use of the Firm's resources. Potential violations of this Policy that come to the Firm's attention during these and other activities may be acted upon.

Users must not send e-mail messages containing unusually sensitive information over the Internet without using an encryption method approved by the Firm. Furthermore, the Firm must be provided with a copy of all passwords and/or private keys needed to decrypt the communications.

VII. SANCTIONS

Potential violations of this Policy may result in suspension of the User's access to the Firm's Internet and e-mail resources, followed by review of any costs and/or charges incurred by the Firm.

Violations of this Policy may subject Users to the loss of Internet and e-mail privileges and may result in disciplinary action, including termination.

Illegal acts involving the Firm's Internet and e-mail resources may also subject violators to prosecution by local, provincial, and/or federal authorities. Suspected law violations may be referred to police agencies. The Firm may seek legal action against any violators, including damages, indemnification and costs.

User's acknowledgement

I acknowledge that I have read, understand and agree to comply with this Internet and E-mail Use Policy as set forth above. I understand that failure to comply with this policy may result in disciplinary action, including termination, as well as legal action against me to seek damages, indemnification and costs.

_____ _____

Name Date

Additional Resources

"Client confidentiality in the digital age." Published by the North Carolina Bar Association. June 20, 2008.

"Computer malpractice is easier than ever." Published by GP Solo. Available at: http://www.abanet.org/genpractice/magazine/2007/jun/computermalpractice.html

"e-mail netiquette for lawyers." Published by NYSBA Journal. Available at: http://ssrn.com/abstract_id=1515812

"Ethical and Risk Management issues in the e-mail era." Privratsky, Mark R. 2005.

The Lawyer's Guide to Records Management and Retention. Published by the American Bar Association. Available at www.abanet.org or by phone at 800.285.2221; product code 5110574. Price is $99.95 regular or $89.95 for members of the ABA Law Practice Management Section.

"Managing the Security and Privacy of Electronic Data in a Law Office." Published by practicePRO. Available at: http://www.practicepro.ca/practice/ElectronicDataSecurity.asp

"Smartphone Ethics and Security." Published by www.myrisk411.com. Available at: http://www.myrisk411.com/Home/tabid/160/EntryId/22/Smartphone-Ethics-and-Security.aspx

Available in the Lawyers Mutual Lending Library

Android Apps in One Hour for Lawyers by Daniel J. Siegel

Cloud Computing for Lawyers by Nicole Black

E-Lawyer: A Guide to Legal Practice Leadership in the Internet Age by Adam Newhouse

Encryption Made Simple for Lawyers by David G Ries, John Simek and Sharon D Nelson

Google for Lawyers by Carole A Levitt & Mark E Rosch

Google Gmail and Calendar in One Hour for Lawyers by Carole A. Levitt and Mark E. Rosch

iPad Apps in One Hour for Lawyers by Tom Mighell

Locked Down: Information Security for Lawyers David G Ries, John Simek and Sharon D Nelson

The Lawyers Guide to Microsoft Outlook 2013 by Ben M. Schorr