Digital File Management – Practice Tips

Many lawyers are attempting to reduce the amount of paper used in their law practices by moving to an electronic/digital file system. The requirements set out by the *Rules* and/or *Code of Ethics* apply equally to paper and electronic files. While there are many ways to keep a file (whether paper or electronic) we have attempted to set out some of the major considerations and/or best practice tips.

Objective: The objective is to establish a best-practice for firms who wish to have a complete and readily accessible electronic record of a client matter. The goal of such a best-practice is to ensure that the files are securely and reliably stored, are retained in electronic formats that are well supported and will be compatible with others if the files are exchanged, and that the files will be readily accessible to another lawyer if the need arises.

Office Systems and Hardware

- Word processing and Document exchange:
    - The word processing system chosen should be one that is in common usage and readily capable of conversion to other common programs. **Microsoft Word** is the most common word-processing program used by law firms and a very commonly used format for exchange of editable documents. For this reason, when exchanging word processing files, the sender and recipient should have the ability to produce and edit and print MSWord documents.
    - If the recipient is expected to edit the document, the original word-processed file may be exchanged. The sender should be careful to ensure that the document does not contain and reveal earlier versions of the documents or comments that may be confidential or subject to solicitor and client privilege.
    - When exchanging documents that do not require editing, PDF (Portable Document Format) format is recommended. A law office should have the ability to create and view PDF files, which is the *de facto* standard for document portability and exchange.
    - When sending a file, the lawyer should be aware of the ability of the recipient to edit the document. The lawyer should ensure that the recipient knows the format that the file is in and whether the recipient will be able to make changes.
    - A document may need to be secured to prevent tampering (consider need for passwords or locking the file using the application software with which the document is accessed).
    - The lawyer may wish to ensure that any changes are tracked. This may be done in MSWord using version tracking. Be careful with use of version tracking, since when it is turned on, previous versions may be accessible to the recipient.
    - Advanced considerations: When is deletion appropriate? What metadata should be preserved?

- Email program:
    - Email programs such as MS Outlook, Mozilla Thunderbird, or other well supported email programs are recommended for office computers.
    - If the lawyer is accessing email on their smart phone, they should be careful to ensure that the email program they are using (e.g. Apple iPhone, Apple Mail, Android,) will synchronize with their desktop office computer to ensure that emails that are received and sent using the smartphone are also retained on the lawyerôs office computer system.
    - Hotmail or Gmail or other such popular free third-party email servers should not be used as the sole means for accessing and retaining practice-related emails. Such servers will not ensure that client confidentiality and solicitor-client privilege is protected.
    - It is recommended that all users in the office use the same email program. If a lawyer chooses to use an email program that others in the office do not use, there should be someone else in the office who is familiar with that program so that the lawyerôs emails can be accessed if he/she is incapacitated.
    - Consideration to be given to what format emails will be saved in. Users should be aware that saving an email in a native format (such as an Outlook .msg or .eml file) does not make the email file accessible to users not equipped with that program.
    - Saving emails in printed form or PDF format only does not preserve the routing data that is part of the email message. In some cases, this may be important. For this reason, original emails should be retained in the email program. This may require periodically archiving the emails in your ñInboxò and ñSentòbox.
    - Be wary of communicating via text and if communication does occur by text ensure the text is saved to the electronic file.

- Electronic file formats conversion:
    - An office should have the ability to create and view PDF files and to view/access other kinds of files in the most commonly used formats (video, photo and audio files). Electronic documents may exist in a variety of formats such as photographs (e.g. files with file extensions: .jpg, .tiff, .bmp, .gif, .pdf), text documents (.pdf, .docx, .doc, .rtf), audio files (.wav, .mp3, .mp4), video files (.avi, .mov, .flv, .wmv, .mp4, trm).
    - Advanced Considerations include: Saving all digital records from native format to a universal format such as PDF (e.g. PDF files can include text, photographs as well as audio and video files).
    - Users should be aware that many electronic files contain metadata. All photographs and videos and other files contain metadata that provide technical information about the camera settings, date, gps location etc. relating to the creation of the file. PDF documents also may contain metadata. This information may be lost if the document is converted to other formats.

- Scanner technology
    - If the firm will be converting paper documents to electronic format, the office should have a networked digital copier/printer/scanner that has a high-speed scanner function capable of creating a digital file in PDF and other formats.
    - Advanced considerations include: a high-speed scanner that is capable of creating a text searchable file (a scanner that has built-in optical character recognition - OCR)

- Computer equipment
    - Your system should have an operating system and networking software that is in common usage (most common is Microsoft Windows / Server but some offices may use Apple or Linux or a combination)
    - Reliable storage of digital records
        - The office should implement procedures:
            1. to prevent loss of data in the event of hardware failures or deletion of data.
            2. to avoid loss of data in the event of a catastrophic event such as a fire, flood.
            3. to ensure that data is protected from cyber threats (computer viruses; ransomware and other malware; hackers)
        - Disk redundancy is useful in preventing loss of data in the event of hardware failures. This can be achieved by users storing client files and office data on multiple redundant network drives (RAID). This makes it much less likely that the office will experience loss of data due to hardware failure.
        - Regular back up procedures should be implemented so your office will be in a position of restoring all office functions in the event of loss of data. Daily backup of critical office accounting data should be done. Backup of client matter files may be less frequent particularly if paper copies are retained. Backup copies stored within the physical office may not survive a catastrophic loss. Remote backup using secure cloud sites may be considered and/or physical off-site storage may be considered.
        - Client files that are being worked on can be backed up automatically as they are saved. This requires configuring the word processor correctly.
        - Backups must be set to run automatically to ensure they are done correctly and regularly.
        - The firm should ensure that the backup system is regularly checked manually to verify that the backups have run.
        - The firm should restore a complete set of backups periodically to verify that all important data/files are being backed up and can be restored.
        - Backup types: Offsite backup site; cloud; external hard drive; USB; (store off site)
    - Redundancy of backup copies ï the firm should ensure that backups are retained for a sufficient time before being deleted and that periodic archiving of backups is done. At any given time, a complete set of the most recent backups should be available.
    - Onsite accessibility ï is the backup easily accessible at the office?

- Offsite accessibility ï where is it stored; how can you access it; is it secure?
- Decommissioning ï the firm should have procedures that ensure data is removed (wiped) before devices containing client information are discarded. This includes all hard drives INCLUDING the hard drive contained on the office photocopier!

File Organization

- All electronic files relating to a client matter should be appropriately named and should be stored in appropriately named folders and sub folders.
  - Files should be saved chronologically by having the file name begin with the date. The YYYYMMDD (or YYY-MM-DD) date format must be used to ensure that alphabetical sorting by filename will result in chronological sorting.

- Naming conventions
  - The firm should ensure consistency across all matters, including file naming conventions and directory structure
  - Consider an add on program for naming/saving message (e.g. Microsoft outlook message save manager)
  - (see above) Date format YYYYMMDD to have files stored in chronological order. Using an underscore (ñ_ò) as the first character will place file at the top of list
  - File names should provide information about the content (e.g. 20161213_Letter_to_client.docx)
  - Be aware of file naming limitations. For example, in Windows, the maximum file name length is 260 characters, and this includes the file path

- Directory (Folder) structure
  - The directory or folder structure should be readily understandable to others. Folders should use nested directories such as Client → matter → subfolders. Example:

Clients>
Doe_John>
Small Claims Action>
Billing>
2016-11-01 Interim Account.pdf
2016-12-30 Final Account.pdf
Correspondence>
2016-12-01 Letter to client setting out retainer.docx
2016-12-03 Email ABC to XYZ setting up case.pdf
Management conference>
2016-12-15 Settlement Agreement.docx
Pleadings>
2016-12-02 Small Claims Summons.docx

Document Management

Consideration may be given to implementing a firm-wide system for document management. This may be more important in the larger firms. Best practice would have everyone in an office managing documents in the same way. Care should be taken to ensure that any software used to manage the document management system is widely used, is well-supported and will continue to be well-supported in the future.

Multiple folders and subfolders can be created. Consider having a õdraftsòfolder in addition to the folder containing the completed document.

Archiving and file retention

- The office may wish to have a procedure for closing digital files e.g. moving digital client files to a location on the system other than the location for current files.
- Storage period ï the same rules that apply to paper files apply to digital files. Given electronic storage is cheap, the firm may not feel the need to destroy digital client files. If the firm wishes to destroy digital files it should develop a policy as to when and how this will be carried out.
- Storage medium ï will the storage medium maintain its integrity for the entire storage period? Will it continue to be accessible?
- The office should periodically do an audit of the integrity of stored records