THE LAW SOCIETY OF NEW SOUTH WALES

Guidelines for Management and Storage of Digital Documents

1. Purpose and scope

The purpose of these guidelines is to establish consistent, secure and compliant practices for the management and storage of digital documents. They are designed to:

a) support lawyers and law practice staff in meeting their professional, ethical and regulatory obligations including confidentiality, privacy laws, data integrity and retention requirements; and

b) enhance efficiency, reduce risk and ensure that legal records are properly maintained, accessible and protected throughout their lifecycle.

2. Summary of requirements

a) An original client document may be in electronic or paper format. A client is entitled to the original format of their document on completion or termination of an engagement.[1]

b) Where a client requests for the original file to be returned, the solicitor should keep a copy at their own expense. It is recommended that a clause to this effect be included in the retainer.

c) If not returned to the client at the completion or termination of the retainer, a solicitor has to retain client documents in its original form for at least seven years[2] after the termination or completion of the retainer.[3] If, however, the solicitor prefers to store the original client documents in electronic format, the solicitor should obtain the client's consent, which can be done by:

   I. adding a clause in the retainer to this effect, or

   II. getting subsequent consent from the client.

   The solicitor should ensure that scanned versions of documents are in a searchable format.

d) If client documents have not been returned to the client, a solicitor can destroy those documents after a period of seven years has elapsed from completion or termination of the engagement, except where there are client instructions or legislation to the contrary.[4]

e) Files consist of both client documents and solicitor documents. The client is only entitled to the former, although a solicitor may choose to provide the entire file at the solicitor's expense.

   As a general rule, a document belongs to the client if it is for the benefit of the client or they have been charged for it. Useful cases on the distinction include *Wentworth v de Montfort (1988) 15 NSWLR 348 and Alexiou v Alexandra White & Ors t/as HWL Ebsworth Lawyers* [2021] NSWSC 485.

---

[1] *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (NSW) rule 14.1.
[2] Some information for example, notes or advice relating to binding financial agreements and Wills may need to be retained for longer.
[3] *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (NSW) rule 14.2.
[4] Ibid.

3. Safe custody documents

Safe custody documents (including wills and deeds) are the exception and should not be digitised or destroyed. These documents must be retained in their original form.

Safe custody documents must either be:

a) retained by the law practice; or

b) returned to the client; or

c) transferred to another law practice, in accordance with rule 6 of the *Legal Profession Uniform Legal Practice (Solicitors) Rules 2015*; or

d) continue to be held in safe custody by the former principal/s of the former law practice or their legal representative if the former principal/s are deceased.

A centralised safe custody register should be kept and maintained in a secure place, separately from the safe custody documents themselves.[5]

The Law Society of NSW's Compliance Review toolkit provides further guidance on management of safe custody documents, including the requirement to have a policy for carrying out an annual safe custody audit.

For further guidance on solicitor obligations when transferring client documents, including safe custody documents, refer to the Law Society of NSW's Practice Checklist.

4. Practical steps

This section sets out some practical steps that law practices can follow when setting up processes to digitise files.

a) Review your retainer and costs agreement to ensure inclusion of the following:
    I. the client's consent to store their document's digitally noting, if relevant, whether the originals will be destroyed; and
    II. at completion or termination of the engagement, all documents will be given to the client in digital form.

b) Build in processes in your practice to ensure that the client understands the implications of a) above.

c) Consider any back up files required as best practice including updating any Record Retention Policy. Note that rule 14 of the Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015 does not apply to copies of the client's documents or solicitor documents. Backing up a file is best practice risk management for a practice, which will be helpful in any Lawcover claim.

d) When storing information, consider file format and acceptable document types. For example:
    I. **PDF** or **PDF/A** for court submissions and finalised documents,
    II. **DOCX** for drafts and editable formats, and
    III. **XLSX** or **CSV** for structured data.

[5] *Legal Profession Uniform General Rules 2015*, rule 94.

e) Set up the system to ensure that:
    I. information is in searchable format. Avoid using scanned images or non-searchable PDFs where text access is needed,
    II. email attachments are saved in native or PDF format, and
    III. meta data is preserved by retaining electronic documents (including emails) in their original or native format.

f) When setting up processes for destruction, consider whether files need to be kept for a period longer than seven years after termination of engagement due to:
    I. type of matter or the type of documents in the file. For example, an instruction sheet for a Will or binding financial agreement notes and advice,
    II. any applicable statutory limitation period,
    III. possible tax implications,
    IV. a live claim,
    V. any Legal Professional Privilege considerations, and
    VI. age of the client, for example, where the client is a minor and the solicitor wishes to keep the file for seven years *after* the minor turns 18.

g) Consider agreement(s) with cloud-based legal practice management software provider (e.g. LEAP or other provider) to ensure that information is capable of being retrieved, searched and/or transferred on retirement, death (e.g. for a sole practitioner) or sale of business.

h) Check that internal policies are up to date, including, for example, Record Retention Policy, Disaster Recovery Plan, and Data Breach Response Plan (see below for further information).

5. Record Retention Policy

Maintain a Record Retention Policy (or similar document) that reflects legal, regulatory, and professional requirements. At a minimum, it should cover the following:

a) the firm's approved Document Management System (**DMS**) or cloud-based platforms which are compliant with data privacy and legal practice standards,

b) any confidentiality undertakings with clients or courts,

c) information that is subject to Legal Professional Privilege,

d) practices relating to the storage of legal files on personal devices, USBs, or unapproved cloud platforms (e.g., Dropbox, Google Drive), including what is prohibited,

e) naming conventions that will ensure searchability and retrievability,

f) system for segregating archived documents from active files,

g) process when transferring files to another practice, which must comply with rule 6 of the *Legal Profession Uniform Legal Practice (Solicitors) Rules 2015*,

h) Access and security controls, including for example:
    I. whether sensitive files are to be encrypted, password-protected, contain multi-factor authentication for accessing all systems containing client information,
    II. access protocols, and
    III. audit trails,

i) any requirements for remote access and mobile devices for example:
    I. whether access can only be via firm-approved devices which has up-to-date security software,
    II. mandatory use of VPNs when accessing files from external networks;
    III. prohibition on downloading or storing documents on mobile phones or tablets, and
    IV. procedures for lost or stolen devices that must be reported immediately and, if necessary, remotely wiped,
j) when information can be securely destroyed (for example, after the expiry of the retention period, unless subject to ongoing litigation or legal hold), and
k) see other requirements below at [6] - [11].

6. Audit and monitor

Ensure that any Record Retention Policy (or similar document) contains audit and monitoring requirements including:

a) regular audits of document storage practices are conducted to ensure compliance,
b) document access logs are maintained and reviewed periodically, and
c) any non-compliance is addressed under the firm's disciplinary procedures.

7. Training and awareness

Ensure that any Record Retention Policy (or similar document) contains staff training requirements including for example:

a) requiring all staff to complete digital document management training as part of onboarding,
b) requiring all staff to undergo ongoing refresher sessions to be held annually or when systems or laws change, and
c) how any updates to the policy and procedures will be communicated to all relevant staff.

8. Disaster Recovery Plan

Maintain a Disaster Recovery Plan (or similar document) that reflects:

a) how the systems are to be backed up (whether this is daily or at other intervals),
b) any requirements for backup data to be encrypted and stored securely, either offsite or in a secure cloud location, and
c) any steps for restoring access to documents in the event of a system failure.

9. Digitisation of paper records

Where a law firm is looking to digitise paper records, ensure that:

a) this is allowed by the law and internal policies,
b) scanned copies are:
    I. high-quality and legible,
    II. saved as searchable PDFs, and

III. linked to the relevant matter in the DMS,

c) a note of destruction paper is retained if originals are destroyed post-digitisation, and

d) client contracts expressly allow for digitisation and destruction.

See also Safe Custody documents at [3] above. These should not be digitised or destroyed.

10. Breach and incidental reporting

All firms, including small firms are at risk of cyber breaches which can lead to breaches of the *Privacy Act 1988*, loss of confidential and privileged information. Of growing concern are scams, impersonation fraud and email compromise.

Any suspected or actual breach of digital document security must be reported immediately to the firm's compliance officer, IT department or a principal of the firm.

Firms should document their breach response in the firm's **Data Breach Response Plan** (or similar document), including notification to affected clients or regulators where required. See also NSW Law Society cyber security resources on Cyber Security Resources | The Law Society of NSW and Law Cover Cyber-Checklist_LSNSW-and-LCI.pdf, Cyber-Fraude-Brochure_LSNSW-and-LCI.pdf and Lawcover-Cyber-Incident-Procedure-and-Emergency-Contacts.pdf.

11. Reviews and updates

Review your policies and procedures every 12 months or earlier if there are material changes in law, technology, or firm policy.

Nominate the person or position that is responsible for updating and enforcing the policies.

These guidelines were published in October 2025.