THE LAW SOCIETY OF SINGAPORE

GUIDANCE NOTE 3.12.1

[Formerly GN 2013, para 3; Council's Guidance Note 1 of 2006]

STORAGE OF DOCUMENTS IN ELECTRONIC FORM

1. This Guidance Note supplements the Practice Direction of Council on "Storage and Destruction of Documents" which dealt with matters such as the period of retention of documents ('Practice Direction 3.12.1'). The Guidance Note sets out in an answer and question format general guidelines to be considered when law practices decide to store their documents in electronic form.

2. This Guidance Note does not lay down any rigid form or style on how the electronic documents should be stored and in what medium they should be stored.

A. Should I Keep All Clients Documents?

3. The return to clients of documents that belong to them should not be left to be dealt with only upon the termination of the retainer. It is prudent to periodically review and arrange for the return of clients' documents on a regular basis or when the documents are no longer required.

4. All clients must be briefed on the procedure for the storage, return or destruction of documents at the commencement of the retainer or it should be stated in the letter of engagement.

B. Can I Store Documents Photographically or Electronically and Destroy the Originals?

5. All original documents of a client should not be destroyed without the express written permission of the client or owner.

6. Where the retainer has been completed, bill paid, and the client does not wish to have the file returned a law practice may store it on a data storage medium or device (such as a disc or storage drive) and then destroy it per the Practice Direction 3.12.1.

7. When in doubt whether to destroy any document, the client's or owner's written permission should always be sought. If it is not possible to obtain such permission you will have to form a view and evaluate the risk. When seeking the client's or owners' permission to store data electronically and destroy documents, you may wish to reserve the right to make a reasonable charge for preparing copies if they are later requested.

C. What Procedures would be Recommended for the Storage of Original Documents in Electronic or Photographic Formats and then the Originals are Destroyed?

8. The Law Society recommends that a law practice considers the terms of the Evidence Act (Cap 97, 1997 Rev Ed) and the following guidelines before the destruction of the originals:

(a) Written evidence of the destruction of the original and of identification of the copy must always be preserved in case oral evidence is no longer available when needed.

(b) There should be a proper system for:
  (i) identification of each file or document destroyed;

(ii) recording that the complete file or document, as the case may be, has been photographed or stored;
(iii) recording identification by the camera operator of the negatives as copies of the documents photographed or file and format the electronic filed will be stored in; and
(iv) preserving and indexing the negatives or the file.

D. What Procedures should be Adopted for the Storage of Photographically or Electronically Stored Documents?

9. The Law Society recommends that the following guidelines be considered when planning for the storage of photographically or electronically stored documents:

(a) records retained/captured in electronic form must be accurate to ensure it is not lost or altered in any way;

(b) the electronic storage system must have an audit trail to capture all transactions on the said system completely;

(c) the electronic storage system must not allow for editing/alteration/deletion of stored electronic records/images;

(d) there must be reasonable image and data security, backup and recovery measures to ensure that the electronic record/image and other data associated to it can be retrieved;

(e) there must be checks/validation to ensure that the indexing of electronic data/images is accurate;

(f) electronic records/images must remain retrievable in the event of a change/upgrade of IT systems or vendors;

(g) there must be precautions in place to prevent unauthorised changes and modifications;

(h) the electronic storage system must be able to provide for complete display and printing of all information associated with an electronic record/image; and

(i) there must be internal controls adequate to ensure reliability, integrity, accuracy, completeness and availability of the electronic storage system.

E. Outsourcing of Storage Systems

10. Before commencing on outsourcing, the following risks of outsourcing electronic storage systems should be considered and evaluated:

(a) due diligence should be carried out to determine an outsourcer's viability, capability, reputation, track record and financial strength;

(b) all outsourcing arrangements be appropriately documented by means of a written outsourcing agreement;

(c) confidentiality of client information must be protected by entering into non-disclosure agreements or confidentiality clauses and using outsource partners in jurisdictions that generally uphold such agreements and clauses;

(d) outsourcing agreements must be terminable in the event that the outsourcing partner:
    (i) goes into liquidation, receivership or judicial management, becomes insolvent, or undergoes change in ownership;
    (ii) has breached confidentiality; or
    (iii) has demonstrated deterioration in the ability to safeguard confidentiality of customer information.

Date: 1 June 2018

THE COUNCIL OF THE LAW SOCIETY OF SINGAPORE