Retention and destruction Policy

Introduction

We owe a number of duties in relation to the retention and destruction of records/documents, in any format, which come into our possession or control or are produced in the course of business. We are committed to complying with those duties by retaining such records/documents securely and ensuring that they are destroyed in a timely and secure manner.

Definitions

"documents" includes, but is not limited to:

- communications between us, our clients and third parties instructed on our clients' behalf;
- documents produced by us in order to achieve the objective of the retainer (for example, agreements or written representations);
- documents prepared by a third party during the course of the retainer (for example, opinions of counsel and experts' reports);
- attendance notes and internal memoranda;
- time recordings;
- drafts and working papers;
- internal emails and correspondence created during the course of the retainer;
- accounting records, including vouchers and instructions.

"deeds" means both deeds within the narrow legal meaning and also any other documents which must be stored in safes or strong rooms when we are not working with them.

"information" includes, but is not limited to: "documents" and "records" as defined in this procedure which may or may not include hard copy documents in any format, electronic documents in any format.

"records" includes, but is not limited to:

- medical records
- personnel records
- occupational health records
- financial records
- educational records
- social care records.

"retention period" – refer to our Retention Schedule.

Background

We have duties under legislation and/or regulations to retain records/documents for certain periods of time, for example under the Limitation Act 1980 and the Money Laundering Regulations 2017. We also have other retention obligations to our indemnity insurers, regulators, accreditation bodies and clients. Balanced against this, the data protection legislation only permits us to retain information including or comprising personal data for as long as is necessary. There are also cost implications of retaining

records/documents for any longer than required and/or retaining duplicate records/documents.

Retention periods

Records/documents must be stored in accordance with this policy and our Sending Confidential Information Sending, Handling and Storing Confidential Information Policy Guidance. Our Retention Schedule provides guidance on retention periods.

We will hold records/documents for all client matter types for a minimum of 7 years from the date of file closure, unless our contract with the client or relevant legislation says otherwise or the fee earner determines that a different period applies as per the Retention Schedules.

Clients are informed of our Retention & Destruction Policy in our Terms of Business.

We may exercise a lien over any records/documents in our possession until all fees, disbursements and other expenses are paid in respect of all matters we have carried out on the client's behalf. If guidance is required on exercising a lien, please contact the Risk & Compliance team.

Storage of information

Records/documents may be held electronically and/or manually and may contain information from any of the categories below (this is not an exhaustive list): -

- Administrative records including: HR, estates, financial and accounting
- (e.g. budget information, annual report information);
- Information concerning complaint handling;
- Manual (e.g. telephone messages, working papers);
- Printouts of audit trails from computer/automated systems;
- Microfiche;
- Audio tapes, cassettes;
- Video tapes, CD-Rom;
- Computer media e.g. CDs, memory sticks;
- Computer output e.g. paper printouts;
- Medical records held on slides, CTG traces

Storage of hard copy and electronic records must be managed in line with this policy and the following policies/procedures:

- Information Security Policy
- Data Protection Policy
- File Management Procedure
- File Management Policy: file closure
- Sending, Handling and Storing Confidential Information Policy

Hard copy records/documents

All hard copy records/documents must be entered on icompli and must be stored in designated tambours across the offices or in accordance with Business Operations

document storage policy. Hard copy documents received from external sources must be scanned into the relevant electronic file on receipt and named so that they can be easily identified.

Hard copy records/documents which are rarely used, or records/documents which are no longer in active use but we need to retain, must be sent to our off-site storage provider by placing a collection request on icompli.

Electronic records/documents

Electronic records/documents must be stored on Filesite, the relevant CMS or BJ Access. Where records need to be retained offline on CD, DVDs, magnetic discs or other removable media, these must be kept in an encrypted format and/or in a designated/controlled access location. Where we receive information in one of those formats it must be scanned into the relevant system/electronic file on receipt and named so that it can be easily identified.

Backup tapes (such as Tape, Disk, and Cartridge) MUST be stored at an authorised secure off-site archive facility whilst not in use.

Monthly, a full set of backup tapes WILL be retained at an authorised secure off-site archive facility for compliance, legal and regulatory purposes.

All backup servers, tape drives and backup tapes MUST be located in a physically secure location with an appropriate level of physical and environmental protection, including authorised access control. The location of the authorised secure off-site archive facility should be of sufficient distance from our offices as to not be impacted or affected by natural disasters or man-made incidents at any of these offices. The best practice distance is 50 miles.

Encryption Requirements

Backup tapes MUST be encrypted in accordance with the Cryptography Policy and applicable Encryption Guidelines.

Data sent to our MFDs (e.g.print jobs, address book contacts etc) is encrypted via an algorithm, as part of the 'Secure erase level 30' service Ricoh (our 3rd party supplier) provides to us. The algorithm key to decrypt the data is securely contained and cannot be altered outside of our network. As such, if the hard drive from the MFD was stolen, the data would be unreadable.

Backup media should be tested regularly, using the established restoration procedures, to ensure that both the media and the procedures are reliable, these testing arrangements shall be aligned to and support our business continuity arrangements.

Original records/documents

Whenever possible, we must not retain original records and documents. We scan original records/documents and return them to the client or sender as soon as practicable, unless we have agreed to retain the originals. If we have agreed to retain original records/documents such as deeds and original signed agreements, they must be stored in accordance with Business Operations Document Storage policy.

Destruction of records/documents

The destruction of records/documents is an irreversible act. Many of the records we hold contain sensitive and/or confidential information and their destruction must be undertaken in secure locations and proof of secure destruction may be required. Destruction of all records, regardless of the media, must be conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure.

Hard copy records/documents

- See Confidential waste policy

Electronic records/documents

- Clearing
- Purging
- Disintegration, Incineration, Pulverisation, and Melting.
- Sanding
- Wiping/overwriting

Any media containing our data must be securely destroyed and proof of secure destruction obtained. Any hard drives from firm laptops, servers, desktop PCs or other equipment that the firm are returning to a supplier or re-selling must be removed from the device and securely destroyed by the firm's chosen destruction third party.

Whilst it is our preference that the destruction of hard drives takes place on our premises, where this is not feasible the third party responsible for the destruction must provide a duty of care note to advise they will ensure the hard drives are securely transported to their premises. Once the destruction has taken place, a certificate must be obtained and retained for auditing purposes.

Items such as network switches and routers that contain network configuration pertaining to our infrastructure must be wiped by an authorised member of the IT team.

Third parties

Third parties instructed by us during the course of our business (for example, counsel and medical experts) have their own obligations in relation to the retention and destruction of records/documents and our letters of instruction remind third parties of their obligations.