Retention and destruction Policy

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, handling and storing confidential information policy. 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.

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:

- Data protection policy
- 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 processes. 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.

Uniflow uses the TLS/SSL encryption standard across port 19100 to send the encrypted print jobs to the machine. The printers have been hardened by forcing them to only use HTTPS. The data sent (E.G - Advanced Box or Mail Box, Address Book data, existing job data, and password information) is saved to the hard disk of the machine which is encrypted by the printer, preventing it from being accessed/readable by unauthorized users. The device also cannot be read or placed into another machine to obtain data should it be removed. The machines are also equipped with the Canon MFP Security Chip, which complies with the FIPS 140-2 Level 2 security standard.

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 processes.

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

Confidential waste

All confidential papers that need to be disposed of should be placed into the confidential bins located around each floor/office. These bins are locked, and only opened when the waste is collected by our external provider. We do however retain copies of keys for these bins within each office in a secure key store/safe should a situation arise where an item is accidently placed into the confidential bin.

Confidential waste collection

We outsource the collection and disposal of confidential waste through an external supplier governed by contractual terms that comply with our information security requirements. Our supplier is contracted to collect the contents of the confidential waste bins and destroy them on site, once a fortnight at each office location as follows:

Birmingham - every Monday
Exeter – every Wednesday
London – every Thursday
Manchester – every Monday
Nottingham – every Friday

In the event that bins become full before the scheduled collection, additional collections are organised.

Retrieval of items mistakenly placed in the confidential waste bins

There may be instances where individuals across the firm need to access the confidential waste bins to retrieve items disposed of in error. In such instances, the following process should be followed:

Between 8am – 6pm:

Please call one of the following, subject to which office you are in:

Nottingham - Please contact the Document Solutions team and ask to speak to a team leader
Birmingham - Please contact the Document Solutions team and ask to speak to a team leader London - Please contact the Document Solutions team and ask to speak to a team leader Exeter - Please contact the local floor captain
Manchester - Please contact the local floor captain

The above points of contact will then seek approval from a third party to allow retrieval of a document from the confidential bin. The third party should be one of the following, subject to the office/department/situation:

- Operations Manager (HAL/IPR)
- Office Head or Deputy
- Exec Board Member or Director
- Managing Partner / Senior Partner

Before 8am / after 6pm:

In the event that you need to retrieve something from the confidential bins out of hours, please email the Business Operations service desk and your request will be sent on to the correct point of contact so that they can action this as soon as someone is in the office.

Full confidential bins

In the event that you notice a confidential waste bin is full or overflowing please email the Nottingham Document Solutions team (regardless of office) so that we can arrange for the bin to be emptied.

Disposal of large quantities of confidential information

In the event that employees need to dispose of a large volume of confidential documents, please contact the Nottingham Document Solutions team (regardless of office) so that we can arrange for secure bags to be provided so that you can dispose of the documents.

Keeping iCompli/records management data up to date

In the event that you place documents into the confidential waste bins that are recorded onto icompli, please remember to delete any such items from iCompli.

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.