We owe a number of duties in relation to the retention and destruction of records, documents and information, 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 data securely and ensuring that they are destroyed in a timely and secure manner.

Definitions

Documents

-
- 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 inte

Deeds any other documents which must be stored in safes or strong rooms when we are not working with them.

Information

occupational health records

- financial records
- educational records
- social care records

Retention Period	refer to our Retention Schedule.

Background

We have legal and regulatory duties 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

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 will 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

All laptops are encrypted as part of our standard build using Bitlocker with TPM. If there is a requirement to use an external storage device, the device must be encrypted. Guidance on encryption and the secure transfer of data is provided to staff in our Sending, Handling & Storing Confidential Information Policy and our IT Encryption Procedure.

Backup media are encrypted in accordance with the Cryptography Policy and will 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 do 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 will 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.

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 isch floor/office. These l

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.

In the event that bins become full before the scheduled collection, additional collections can be organised via the Document Solutions Team.

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 individual will contact the Document Solutions team leader or local floor captain, as applicable for their office, who will seek approval froma member of senior management. Out of hours requests will be directed to Business Operations service desk for action as soon as someone is in the office.

Disposal of large quantities of confidential information