Data Retention and Disposal Policy

Introduction

In the course of carrying out various functions, we create and hold a wide range of recorded information. Records will be properly retained to enable us to meet our business needs, legal requirements, to evidence events or agreements in the event of allegations or disputes and to ensure that any records of historic value are preserved.

The untimely destruction of records could affect:

- the conduct of business;
- the ability of the business to defend or instigate legal actions;
- the business's ability to comply with statutory obligations; and/or
- the business's reputation.

Conversely, the permanent retention of records is undesirable and, in certain circumstances, unlawful. Therefore, disposal is necessary to free up storage space, reduce administrative burden, and to ensure that the organisation does not unlawfully retain records for longer than necessary, particularly those containing personal data.

This policy supports our organisation in demonstrating accountability through the proper retention of records and by demonstrating that disposal decisions are taken with proper authority and in accordance with due process.

Purpose

The purpose of this policy is to provide guidance as to set out the length of time that records should be retained and the processes to review the records as to any further retention or for disposing of records at the end of the retention period. The policy helps to ensure that we operate in compliance with the General Data Protection Regulation and any other legislative or regulatory retention obligations.

Scope

The policy covers the records listed in the Data Processed Register, irrespective of the media on which they are created or held, including:

- paper;
- electronic files (including database, Word documents, power point presentations, spreadsheets, web pages and e-mails); and

- photographs, scanned images, CD-ROMs, and videotapes.

The policy covers all types of records that we create or hold which may include but are not limited to:

- employee data;
- client data;
- minutes of meetings;
- data from external parties;
- contracts and invoices;
- registers;
- legal advice;
- file notes;
- financial accounts; and
- the organisation's publications.

Application

The policy applies equally to all permanent and casual employees, agency staff, and outsourced suppliers.

Minimum Retention Period

Unless a record has been marked for 'permanent preservation' it should only be retained for a limited period of time. A recommended minimum retention period is provided for each category of record in the Data Processed Register. The retention period applies to all records within that category.

The recommended minimum retention period derives from either:

- business need;
- legislation;
- responding to complaints;
- taking or defending legal action

The case records held on our case management software system are regularly cleansed of any personal data. All cases that are over 15 years from completion, are selected for a GDPR audit and deletion. Individual barristers review their cases and confirm in writing if any cases must be kept any longer, in line with their own personal data deletion policy. All cases that concern children are in the main, retained for over 21 years.

The current agreed data retention periods are set out in Appendix 1.

Disposal

The Data Protection Officer is responsible for ensuring that data is periodically reviewed (at least annually) to determine whether any retention periods have expired. Once the retention period has expired, the data must be reviewed and a disposal action agreed upon.

A disposal action is;

- the destruction of the data; or
- the retention of the data for a further period; or,
- alternative disposal of the data.

The disposal action decision must be reached having regard to:

- on-going business and accountability needs (including audit);
- current applicable legislation;
- whether the data has any long-term historical or research value;
- best practice in the business industry;
- costs associated with continued storage versus costs of destruction; and
- the legal, political, and reputational risks associated with keeping, destroying or losing control over the data.

Decisions must not be made with the intent of denying access or destroying evidence.

Destruction

No destruction of data should take place without assurance that:

- the data is no longer required by any part of the business;
- no work is outstanding by any part of the business;
- no litigation or investigation is current or pending which affects the data; and
- there are no current or pending Freedom of Information or Data Protection access requests which affect the data.

All disposals are recorded on the Data Disposal Record, see Appendix 2.

Destruction of Paper Records

Destruction should be carried out in a way that preserves the confidentiality of the data. Non-confidential data can be placed in ordinary rubbish bins or recycling bins. Confidential data should be placed in confidential waste bins or shredded and placed in

paper rubbish sacks for collection by an approved disposal firm. All copies, including security copies, preservation copies and backup copies, should be destroyed at the same time and in the same manner.

Destruction of Electronic Records

All electronic data will need to be either physically destroyed or wiped in keeping with the organisation's Security Policy. Deletion of the files is not sufficient.

The case records held on our case management software system are regularly cleansed of any personal data. All cases that are over 15 years from completion, are selected for a GDPR audit and deletion. Individual barristers review their cases and confirm in writing if any cases must be kept any longer, in line with their own personal data deletion policy. All cases that concern children are in the main, retained for over 21 years.

Further Retention

The data may be retained for a further period if it has on-going business value or if there is specific legislation that requires it to be held for a further period. Data should not ordinarily be retained for more than 30 years in aggregate from the date of creation, save for human resources information that may need to be retained for 100 years from date of birth.

Further Information

This document should be read in conjunction with the Data Protection Policy and Data Security Policy.

Appendix 1

Data Retention Periods

Data Type	Retention Period	Rationale
Employee Data	End of employment + 6 years	Legal & Financial obligation
Customer Data	Duration of case + 6 years	Legal Obligation
Organisational Data	Duration of case + 6 years	Legal & Finance Obligation
Contractor Data	Duration of contract + 6 years	Legal & Financial Obligation

Appendix 2

Data Disposal Record

Data Type	Disposal Date	Disposal Method	Rationale
Employee Data			
Customer Data			
Organisational Data			
Contractor Data			