Retention of Records Procedure

Overview

This procedure has been developed to ensure effective retention of records in line with the relevant data protection laws and regulations. We will only retain the specific data required for processing, and will only retain this data for as long as is necessary to serve its specific purpose.

This procedure applies to all records we hold, including:

- All electronic media;
- Online records;
- Paper-based records.

The basic procedure for building a retention schedule (as part of building our information inventory) is as follows:

- Identify all data in the organisation;
- Identify where this data is held and by whom (including third parties);
- Describe the purpose of this data (i.e. the basis for retention);
- Define the retention period, inc when this starts;
- Provide justification for the retention period;
- Describe the disposal method; and
- Identify who manages the data.

Procedure

The procedure will be followed in line with the guidance below:

Storage of Records

Records will be version controlled, with the minimal number of versions stored, ideally one version where possible. Sensitive information will be protected either via password or encryption.

Electronic information will be stored only on agreed servers/hardware.

Paper copy records will be locked in a secure location when not being used.

In order to provide the appropriate level of service, we may need to share some personal data with third parties. These arrangements are summarised in our Privacy Notice and

detailed in our data inventory. This sharing will only be for the specific purposes agreed and will be carried out under the appropriate data processing /confidentiality agreements. This will include the third party making adequate provision for secure storage of records, and a clear approach to retention.

Where data will be held outside of the UK or European Economic Area, we will ensure the appropriate safeguards in place, examples include (see Data Protection Policy for more detail):

- Adequacy decision
- Privacy Shield
- Binding Corporate Rules
- Model Contract Clauses

Destruction of Records

Destruction of data will be handled as follows:

- Electronic media – disposed of using a certified agency that disposes of electronic devices.
- Online records – (stored in all applications) are deleted with all backup records subsequently removed.
- Paper-based records – shredded or disposed of via a certified secure shredding organisation.

Destruction of data must be completed within 30 days of a retention period expiry.

Roles and Responsibilities

The following roles are responsible for the retention of these records as they are the information asset owners:

- Data Managers are responsible for ensuring that all personal data under their charge is collected, retained and destroyed in line with the requirements of the GDPR, including deletion of records past their retention period.
- Data Protection Representative is responsible for ensuring compliance with this procedure, as well as periodically reviewing its effectiveness.
- The Executive is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

Review of this Procedure

This procedure and the supporting Retention Schedule will be reviewed by the Data Protection Representative on at least an annual basis to ensure is accuracy and effectiveness.