Data Retention Policy

Date	**24th January 2018**
Reviewed	**22nd June 2020**
Date of next review	**July 2021**

Data Retention Policy

Data Retention Policy

1. Purpose, Scope, and Users

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within Autism Bedfordshire ("the Charity").
This policy applies to all divisions, processes, and organisations in all areas in which the Charity operates and has dealings or other business relationships with third parties.
This policy applies to all trustees, employees, volunteers, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this policy and ensure adequate compliance with it.
This policy applies to all information used at the Charity. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio
- Data generated by physical access control systems

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection Policy
- Storage, Handling , Use, Retention & Disposal Of Disclosures & Disclosure Information Policy - Revised March 2018

3. Retention Rules

3.1.Retention General Principle

In the event, for any category of documents not specifically defined elsewhere in this policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

3.2.Retention General Schedule

The Data Protection Officer defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.
As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by the Charity to prove compliance with any legal requirements; or

- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

3.3. Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to the Data Protection Officer.

3.4. Destruction of Data

The Charity and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Charity's Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of the Charity as a result of malicious or unintentional destruction of information – these controls are described in the Charity's IT Security Policy.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

3.5. Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection, the Data Protection Officer, has the responsibility to ensure that each of the Charity's workplaces complies with this policy. It is also the responsibility of the Data Protection Officer to assist with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this policy must be reported immediately to Data Protection Officer. All instances of suspected breaches of the policy shall be investigated and action taken as appropriate.

Failure to comply with this policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Charity's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Charity premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

4. Document Disposal

4.1. Routine Disposal Schedule

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges / external costs;
- Transmission documents such as letters, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value;
- Message slips;
- Superseded address list, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

4.2. Destruction Method

Level 1 documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded) and shall be subject to secure electronic deletion. Disposal of these documents should include proof of destruction.

Level 2 documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and disposed of; electronic documents will be subject to secure electronic deletion.

Level 3 documents are those that do not contain any confidential information or personal data and are published Charity documents. These should be strip-shredded or disposed of through a

recycling Charity and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

5. Managing Records Kept on the Basis of this Document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Retention Schedule	**Data Protection Officer's Google Drive**	**Data Protection Officer**	**Only authorized persons may access this document**	**Permanently**

6. Validity and document management

This document is valid as of January 2019.

The owner of this document is the Data Protection Officer who must check and, if necessary, update the document at least once a year.

7. Appendices

Data Retention Schedule

Financial Records

Personal data record category	Mandated retention period	Record owner
Payroll records	Seven years after audit	Finance
Supplier contracts	Seven years after contract ends	Finance
Chart of Accounts	Permanent	Finance
Fiscal Policies and Procedures	Permanent	Finance
Permanent Audits	Permanent	Finance
Financial statements	Permanent	Finance
General Ledger	Permanent	Finance
Investment records	7 years	Finance
Invoices	7 years	Finance
Cancelled cheques	7 years	Finance
Bank deposit slips	7 years	Finance
Business expenses documents	7 years	Finance
Cheque registers/books	7 years	Finance
Property/asset inventories	7 years	Finance
Credit card receipts	3 years	Finance
Petty cash receipts/documents	3 years	Finance

Business Records

Personal data record category	Mandated retention period	Record owner
Article of Incorporation to apply for corporate status	Permanent	Finance
Board policies	Permanent	Finance
Board meeting minutes	Permanent	Finance
Tax or employee identification number designation	Permanent	Finance
Office and team meeting minutes		Finance
Annual corporate filings	Permanent	Finance

HR: Employee Records

Contracts

Personal data record category	Mandated retention period	Record owner
Signed	Permanent	Finance
Contract amendments	Permanent	Finance
Successful tender documents	Permanent	Finance
Unsuccessful tenders' documents	Permanent	Finance
Tender – user requirements, specification, evaluation criteria, invitation	Permanent	Finance
Contractors' reports	Permanent	Finance

Operation and monitoring, eg complaints	Permanent	Finance

Customer Data

Personal data record category	Mandated retention period	Record owner
Platform data – inclusive of Video data, comments, attachments, profile picture, email address, first and second name	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 9 months	Customer
Live chat history	Records deleted after 1 year	Support
Screen recordings from support session	Automatically deleted after 90 days	Support
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries, DPO information	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be removed from the back-ups within X months	Support
Metrics data	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be anonymised	Development Team

Non – Customer Data

Personal data record category	Mandated retention period	Record owner

Name, email address	Kept until person unsubscribes / requests to be removed from system	Marketing & Sales
Call recordings	Automatically deleted after 6 months	Sales

IT

Personal data record category	Mandated retention period	Record owner
Recycle Bins	Cleared monthly	Individual employee
Downloads	Cleared monthly	Individual employee
Inbox	All emails containing PII attachments deleted after 3 years.	Individual employee
Deleted Emails	Cleared monthly	Individual employee
Personal Network Drive	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee
Local Drives & files	Moved to network drive monthly, then deleted from local drive	Individual employee
Google Drives, drop box	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee