Data Retention and Deletion Policy

Document Control Table

Policy Title	**Data Retention and Deletion Policy**
Document Reference	ORG/DP/008
Version	1.0
Effective Date	
Next Review Date	

1.0 Purpose and Legal Basis

This Data Retention and Deletion Policy is a core component of the charity's commitment to responsible governance. Its purpose is to establish a clear and consistent framework for managing the lifecycle of information held by the charity. Adherence to this policy is strategically important for ensuring compliance with our legal obligations, managing risks effectively, and protecting the sensitive personal information of our unique beneficiary community, their families, and their descendants.

Legal and Regulatory Framework

This policy is founded upon the requirements of the United Kingdom's legal and regulatory landscape. The charity is committed to upholding its obligations under the following key frameworks:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Equality Act 2010
- The Data (Use and Access) Act 2025
- Relevant guidance from the Charity Commission for England and Wales.

2.0 Scope

This policy applies universally to all operations and activities conducted by or on behalf of the charity. It is designed to ensure that all data and records are handled in a consistent, secure, and compliant manner, regardless of format or location.

Personnel Covered by This Policy

All individuals acting on behalf of the charity are required to adhere to this policy. This includes:

- Trustees
- Volunteers
- Contractors and third-party suppliers
- Any future Staff

Data and Records Covered by This Policy

This policy governs all information created, received, processed, or stored by the charity in the course of pursuing its charitable objects. This includes, but is not limited to:

- **Beneficiary Data:** Grant applications, needs assessments, case files, support records, and communication logs.
- **Research Data:** Anonymised or pseudonymised data gathered for research into the effects of clastogenic exposure.
- **Financial Records:** Invoices, expense claims, bank statements, grant award letters, and annual accounts.
- **Governance Documents:** Trustee meeting minutes, signed policies, Charity Commission returns, and declarations of interest.
- **Contractor and Partner Information:** Agreements, due diligence records, and correspondence.

The policy applies to all formats in which this information is held, including electronic files stored on computers or servers and physical paper records.

3.0 Policy Statement

The charity is committed to:

- Processing personal data fairly, lawfully, and only for the specific charitable purposes outlined in its constitution.
- Retaining personal and corporate data for no longer than is necessary to fulfil those purposes or to meet our legal, regulatory, or operational obligations.
- Applying the principles of data minimisation and storage limitation by ensuring we only collect, process, and store information that is relevant, adequate, and absolutely necessary.

- Ensuring the secure, confidential, and permanent deletion or destruction of data once its mandated retention period has expired.
- Protecting the rights, freedoms, and privacy of our beneficiaries, trustees, volunteers, and partners at all times.

4.0 Definitions

Term	Definition in the Context of the charity
Personal Data	Any information relating to an identified or identifiable living individual. This includes names, contact details, and any other information that can be linked to a person.
Special Category Data	Personal data which is more sensitive and requires higher levels of protection, usually relating to health conditions and finances..
Processing	Any operation performed on data, such as collection, recording, storage, use, disclosure, or destruction.
Retention Period	The specific length of time for which a particular category of data or record must be kept by the charity before it is securely destroyed.
Secure Deletion	The process of destroying data permanently and irreversibly, ensuring it cannot be recovered or reconstructed. This applies to both electronic and physical records.
Data Subject	The identified or identifiable living individual to whom personal data relates. Within the charity, this includes our beneficiaries, their families, our trustees, volunteers, and contractor personnel.

5.0 Procedures

5.1 Data Retention Schedule

The Data Retention Schedule is the charity's authoritative guide for all retention and disposal decisions. Adherence to these periods is mandatory for all personnel to ensure legal compliance and manage risk.

Data Category	Examples of Documents	Retention Period	Justification
Beneficiary & Grant Records	Application forms, needs assessments, grant award letters, case files, and communication logs	7 years after the last contact with the beneficiary	To meet financial audit requirements (HMRC), manage ongoing support, and defend against potential legal claims, which typically have a limitation period of 6 years (Limitation Act 1980).
Research Data	Anonymised or pseudonymised data from research into clastogenic exposure	**Anonymised Data:** Indefinitely. **Pseudonymised Data:** Retained for the necessary research period, subject to a mandatory review every 5 years.	To support the charity's constitutional objects of conducting research (Object 3(2)) and preserving heritage (Object 3(4)). Data that has been fully and irreversibly anonymised falls outside the scope of UK GDPR. Pseudonymised data remains personal data; its continued storage must be justified as necessary for the research or heritage purpose at each 5-year review.
Trustee & Governanc e Records	Trustee meeting minutes, signed policies, Charity Commission returns,	Permanently	To maintain a permanent record of the charity's governance, key decisions, and compliance history, forming the corporate memory of the CIO.

	declarations of interest.		
Financial & Accounting Records	Invoices, expense claims, bank statements, annual accounts, gift aid declarations	7 years from the end of the financial year	To comply with HMRC requirements to keep records for 6 years from the end of the last company financial year, and with the Charities Act 2011 record-keeping obligations.
Contractor & Supplier Records	Contracts, service level agreements, due diligence records, invoices	7 years after the end of the contract	To manage contractual obligations and liabilities, and for financial audit and legal purposes.

5.2 Secure Deletion and Disposal Procedures

Once a retention period has expired, data must be destroyed securely and permanently. The method of destruction must be appropriate to the format and sensitivity of the data.

- **Electronic Data:** Must be destroyed using methods that ensure data is irrecoverable. This includes secure digital erasure using specialist software, overwriting, or physical destruction (degaussing) of the storage media. Simply deleting a file is not sufficient.
- **Physical Data:** All paper records containing personal or confidential information must be destroyed by cross-cut shredding. For larger volumes, a certified confidential waste disposal service must be used to ensure a secure chain of custody and verifiable destruction.

5.3 Exceptions and Legal Holds

In the event that data becomes relevant to a legal dispute, formal investigation, or external audit, the standard retention period may be suspended. The Data Protection Officer must be notified immediately. They will issue a "legal hold" instruction to prevent the destruction of the relevant data until the matter is formally concluded, at which point the standard retention schedule will resume.

6.0 Roles and Responsibilities

- **The Board of Trustees:** Holds ultimate responsibility for this policy. The Board is responsible for formally approving the policy, ensuring it is properly implemented and resourced, and for overseeing the charity's overall compliance with data protection law.
- **The Data Protection Officer (DPO)** is responsible for the operational management of this policy. This includes maintaining and updating the Data Retention Schedule, providing advice and guidance to the Board and volunteers, coordinating secure data disposal activities, and acting as the primary point of contact for all retention-related queries.
- **Trustees, Volunteers, and Contractors:** Are responsible for understanding and adhering to this policy and the Data Retention Schedule in their day-to-day activities. They have a duty to manage the data they handle in accordance with these procedures and to seek guidance from the DPO when unsure.

7.0 Implementation

- **Timeline:** Upon formal adoption by the Board, the DPO will conduct an initial audit of all existing data against the new retention schedule. This review will be completed within the first 6 months to identify and schedule the disposal of data that has already exceeded its retention period.
- **Training:** All Trustees will receive mandatory training on this policy, their legal obligations, and their specific responsibilities within 3 months of its adoption. This training will be recorded in the meeting minutes.
- **Resources:** The Board will ensure necessary resources are made available for compliance. This will include procuring a contract with a certified confidential waste disposal service for the secure destruction of physical records.

8.0 Monitoring, Audit, and Review

- **Annual Review:** The Board of Trustees will formally review this policy and the associated Data Retention Schedule at least once a year. This review will ensure the policy remains aligned with current legislation and the charity's evolving activities.
- **Reporting:** The DPO will provide a concise annual report to the Board confirming that data disposals during the preceding year have been conducted in line with this policy.
- **Compliance Audits:** Compliance with this policy will be subject to periodic internal review to ensure procedures are being followed correctly across all of the charity's activities.

9.0 Related Policies

This policy should be read and understood in conjunction with other key governance documents that form our integrated framework for compliance and risk management. These include:

- Overall Data Protection Policy
- Privacy Policy
- Information Security Policy
- Data Breach Notification Policy
- Subject Access Request (SAR) Handling Policy
- Internal Financial Controls Policy