Overall Data Protection Policy

Document Control

Item	Details
Policy Title	Overall Data Protection Policy
Document Ref.	ORG/DP/009
Version	1.0
Status	Adopted
Effective Date	
Next Review	
Policy Owner	The Board of Trustees

2.0 Purpose and Legal Basis

For the charity, data protection extends beyond a simple matter of legal compliance. It is a fundamental component of our duty of care and the bedrock of the trust we must maintain with our beneficiary community, many of whom are vulnerable. This policy establishes the definitive framework for ensuring that all personal information entrusted to the charity is handled with the highest standards of care, respect, and integrity, reflecting our commitment to the Beneficiary Community we serve.

2.1 Purpose

The core objectives of this policy are to:

- Define a comprehensive, high-level framework for the lawful, fair, and ethical processing of all personal data.
- Ensure the charity's full compliance with all relevant UK data protection legislation and the regulatory requirements of the Charity Commission and the Information Commissioner's Office.
- Guarantee the rights and freedoms of every individual whose personal data the charity processes, including our beneficiaries, trustees, volunteers, and contractors.
- Safeguard the charity's assets and reputation by systematically identifying and mitigating the risks associated with all data processing activities.

2.2 Legal Basis

This policy and all its associated procedures are grounded in and designed to ensure full compliance with the key legal and regulatory instruments governing data protection in the United Kingdom. These include:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018.
- The Equality Act 2010.
- The common law duty of confidentiality.
- All relevant guidance issued by the Charity Commission for England and Wales and the Information Commissioner's Office (ICO).

The practical application of this legal framework across the charity’s operations is defined by the scope of this policy.

3.0 Scope

A clearly defined scope is strategically essential for applying consistent and robust data protection standards across all of the charity's operations. This ensures that a universal standard of protection is afforded to every individual involved with the charity, without exception.

3.1 Who This Policy Applies To

This policy applies to all personal data processing activities undertaken by or on behalf of the charity and is binding on the following individuals and groups:

- **Charity Trustees** of the charity.

- **Volunteers** acting on behalf of the charity.
- **Staff**, if any are employed, as permitted under Clause 4(4) of the Constitution.
- **Contractors** and external service providers working with the charity, such as professional fund managers, are permitted under Clause 4(5) of the Constitution.
- **Beneficiaries**, defined as the "Beneficiary Community" as per Clause 3(1) of the Constitution.

3.2 What This Policy Covers

This policy applies to all personal and special category data that the charity processes, regardless of the format in which it is held (e.g., electronic databases, email communications, paper records) or the physical location where it is stored. This includes all data relating to beneficiaries, trustees, volunteers, and suppliers. The governing principles for all activities within this scope are articulated in the formal Policy Statement that follows.

4.0 Policy Statement

This statement represents the formal and public commitment of the Board of Trustees to ethical data handling. For a charity supporting a vulnerable community, this statement is a primary tool for risk management, designed to build trust with beneficiaries and demonstrate accountability to stakeholders and regulators.

The charity is committed to processing personal data in accordance with its responsibilities under the UK GDPR and the Data Protection Act 2018. We will adhere to the following core principles:

- We will process all personal data **lawfully, fairly, and in a transparent manner**.
- We will collect data only for **specified, explicit, and legitimate purposes** directly related to our charitable objects and will not process it in a manner that is incompatible with those purposes.
- We will ensure the data collected is **adequate, relevant, and limited to what is necessary** in relation to the purposes for which it is processed.
- We will take every reasonable step to ensure personal data is **accurate** and, where necessary, kept up to date, rectifying or erasing inaccurate data without delay.
- We will retain data in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data is processed.
- We will process data in a manner that ensures **appropriate security**, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures.

To ensure a shared understanding of these commitments, the following section provides clear definitions of key data protection concepts.

5.0 Definitions

Precise definitions are vital for the correct interpretation and application of this policy by everyone involved with the charity. This ensures a common and consistent language for managing our data protection responsibilities.

Term	Definition
Personal Data	Any information relating to an identified or identifiable living individual who can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.
Special Category Data	Personal data which is more sensitive and requires a higher level of protection. This includes information about an individual's health, racial or ethnic origin, or genetic data. The charity processes such data, particularly health information, to fulfil its charitable objects for the Beneficiary Community as defined in Clause 3 of its Constitution.
Processing	Any operation or set of operations performed on personal data, whether or not by automated means. This includes collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, dissemination, restriction, erasure, or destruction.
Data Subject	The identified or identifiable living individual to whom personal data relates. In the context of the charity, this includes beneficiaries, trustees, volunteers, and contractors.
Data Controller	The entity that determines the purposes and means of processing personal data. For the purposes of this policy, this is the charity.

Data Processor	A person or organisation that processes personal data on behalf of the Data Controller.
Beneficiary	An individual eligible for support under the charity's objects, as defined in Clause 3 of its Constitution.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

These definitions underpin the operational procedures that translate our policy commitments into consistent and auditable practice.

6.0 Procedures

This section outlines the core operational guidance for the charity. These procedures are designed to translate the policy's principles into consistent, compliant actions and to embed data protection into our day-to-day activities.

1. **Upholding Data Protection Principles:** All personal data will be processed in strict accordance with the core principles of UK GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.
2. **Lawful Basis for Processing:** A valid lawful basis under UK GDPR will be identified and documented for each data processing activity. Where special category data is processed, an additional, specific condition for processing will also be identified and documented.
3. **Data Subject Rights:** The charity will implement and maintain clear procedures to uphold the rights of data subjects, including the right of access, rectification, erasure, restriction, data portability, and the right to object to processing.
4. **Information Security:** Appropriate technical and organisational measures will be implemented to protect personal data from unauthorised access, loss, or destruction.
5. **Data Breach Management:** A robust procedure will be maintained to ensure data breaches are identified, investigated, and, where necessary, reported to the ICO and affected data subjects within the timeframes mandated by law. This directly addresses a critical omission identified in the Gold.pdf governance review.

6. **Data Protection by Design and Default:** Data protection principles will be embedded into all new projects, systems, and processes from their inception to ensure privacy is a foundational consideration.
7. **Third-Party Data Processors:** Rigorous due diligence will be conducted on all third-party contractors who process personal data on behalf of the charity. This replaces the inadequate and non-compliant questionnaire previously identified in the Gold.pdf governance review.
8. **Data Protection Impact Assessments (DPIAs):** DPIAs will be conducted for any processing activities that are likely to result in a high risk to the rights and freedoms of individuals.

For these procedures to be effective, roles and responsibilities must be clearly defined and allocated.

7.0 Roles and Responsibilities

The clear allocation of responsibilities is critical for effective data protection governance and for embedding a culture of accountability throughout the charity.

- **The Board of Trustees:** Holds ultimate responsibility and accountability for ensuring the charity's compliance with data protection law and this policy. This is an integral part of their duty to manage the affairs of the CIO, as defined in Clause 9(1) of the Constitution.pdf.
- **The Data Protection Officer (DPO):** Responsible for monitoring internal compliance with this policy, informing and advising the Board on data protection obligations, and acting as the primary point of contact for data subjects and the ICO. This position is filled by an appointed Trustee.
    - **Managing Conflicts of Interest for the DPO:** The DPO must be able to perform their duties in an independent manner. Any such appointment will be formally documented, and robust mitigation measures will be implemented to ensure the DPO is not responsible for determining the purposes and means of processing data for which they also provide oversight.
- **All Trustees, Volunteers, and Contractors:** Have a personal responsibility to handle the personal data they access in a manner that is compliant with this policy and any associated procedures and training they receive.

This framework of accountability is made effective through the systematic and practical implementation of this policy.

8.0 Implementation

This section details the practical measures that will be taken to embed this policy and its principles into the charity's day-to-day operations, ensuring it functions as a living document that guides our actions.

8.1 Policy Rollout

This policy is effective immediately upon its formal adoption by the Board of Trustees. It supersedes all previous data protection policies, including the flawed V2.0 policy identified in the Gold.pdf governance review.

8.2 Training and Awareness

All trustees, volunteers, and relevant contractors will receive mandatory training on their data protection responsibilities upon induction. Regular refresher training will be provided to ensure ongoing awareness of the charity's policies and any changes in data protection law or best practice.

8.3 Resource Allocation

The Board of Trustees commits to ensuring that adequate resources—including time, financial, and personnel—are made available to support the effective implementation and ongoing maintenance of this policy and its related procedures. The effectiveness of this implementation will be verified through a continuous cycle of monitoring and review.

9.0 Monitoring, Review, and Audit

Ongoing monitoring and regular review are essential governance disciplines that ensure this policy remains effective, compliant, and fit for purpose, creating a cycle of continuous improvement.

9.1 Monitoring and Reporting

The Data Protection Officer (DPO) is responsible for monitoring data protection compliance and will provide a formal report to the Board of Trustees at least annually. Key indicators for monitoring will include the number of Subject Access Requests (SARs) received, their response times, and the number of data breaches or security incidents recorded.

9.2 Policy Review

This policy will be formally reviewed by the Board of Trustees at least annually to ensure its continued relevance and effectiveness. Critically, an immediate review will also be triggered by any significant changes to data protection legislation, the charity's operations, or its data processing activities. This structured review process directly addresses the past failure of policies to remain current, as highlighted in the Gold.pdf

governance review. This policy serves as the foundation of a wider, integrated suite of data management documents.

10.0 Related Policies and Documents

This policy operates as the cornerstone of a comprehensive and integrated data protection framework. It functions in conjunction with a wider suite of specific policies and procedures, the development of which is a strategic priority for building a complete and compliant governance structure.

- Privacy Notice for Beneficiaries and Supporters
- Information Security Policy
- Data Breach Notification Procedure
- Subject Access Request (SAR) Procedure
- Data Subject Rights Policy
- Document Retention and Archiving Policy
- Third-Party Processor Due Diligence Procedure
- Conflict of Interest Policy