Data Protection Impact Assessment (DPIA) Policy

Document Control

Document Title	**Data Protection Impact Assessment (DPIA) Policy**
Document Reference	ORG/DP/011
Version	1.0
Effective Date	
Next Review Date	

1.0 Purpose and Legal Basis

This policy provides the framework for conducting Data Protection Impact Assessments (DPIAs). The DPIA process is not a bureaucratic hurdle but a critical risk management tool that enables the charity to innovate and deliver its services confidently while upholding its profound duty of care to its beneficiaries. By proactively identifying and addressing privacy risks before they materialise, this policy ensures that the charity's activities build and maintain the trust of the Beneficiary Community.

The core purpose of this policy is to establish a clear, consistent, and mandatory framework for identifying, assessing, and mitigating data protection risks associated with any new or significantly changed processing of personal data. It places particular emphasis on activities that are considered high-risk to the rights and freedoms of individuals.

This policy is founded on the following legal and regulatory requirements, which mandate a proactive approach to data protection:

- The UK General Data Protection Regulation (UK GDPR), specifically the legal requirement to conduct a DPIA for high-risk processing as outlined in Article 35.
- The Data Protection Act 2018 supplements and operationalises the UK GDPR within UK law.
- The Equality Act 2010 ensures that data processing activities do not result in unfair, biased, or discriminatory outcomes for any individuals or groups within our beneficiary community.
- The principles of purpose limitation are reinforced by upcoming legislation such as the Data (Use and Access) Act 2025.

This document outlines the scope of activities to which these legal principles and our internal procedures apply.

2.0 Scope

A clearly defined scope is essential for the effective and consistent application of the DPIA policy across all of the charity's operations, ensuring no high-risk activity is overlooked.

This policy applies to all processing of personal data undertaken by the charity, its Board of Trustees, any volunteers, and all third-party contractors or service providers who process personal data on the charity's behalf.

Furthermore, this policy applies to all systems, projects, processes, and initiatives that involve the processing of personal data, from their initial conception and design phase through to their implementation and eventual decommissioning.

This scope establishes the charity's official position on integrating data protection into its operational lifecycle.

3.0 Policy Statement

This policy statement represents the Board of Trustees' definitive commitment to embedding the principles of 'privacy by design and by default' into the charity's culture and operational DNA.

The Board of Trustees for the charity formally declares its commitment to a culture of privacy by design. To this end, the charity will:

- Proactively identify, evaluate, and mitigate data protection risks before the commencement of any new or significantly changed data processing activity.

- Ensure that all processing of personal data, especially that involving the potentially vulnerable members of the Beneficiary Community, is lawful, fair, transparent, and necessary for the achievement of our charitable objects.
- Integrate the Data Protection Impact Assessment process as a mandatory and integral component of all project, system, and process planning and review cycles.
- Uphold and protect the data protection rights and fundamental freedoms of every individual whose personal data we process.

To ensure this commitment is consistently met, it is vital that all parties share a common understanding of the key terms used in this policy.

4.0 Definitions

Establishing clear and consistent definitions for key terms is crucial for ensuring that all Trustees, volunteers, and partners involved in the DPIA process understand their obligations and the specific context of the charity's work.

Term	Definition
Data Protection Impact Assessment (DPIA)	A systematic process designed to identify and minimise the data protection risks of a project or plan. It is a key part of the accountability obligations under the UK GDPR, helping the charity to assess privacy risks to individuals and determine the measures required to mitigate those risks effectively.
High-Risk Processing	Any type of processing that is likely to result in a high risk to the rights and freedoms of individuals. For the charity, this includes, but is not limited to, the large-scale processing of health and wellbeing data. It also includes systematic monitoring or any processing involving the data of our beneficiary community, who may be considered vulnerable individuals.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). This includes identifiers such as a name, an identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Special Category Data	Personal data that is particularly sensitive and requires a higher level of protection. This includes information about an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a person's sex life or sexual orientation. For the charity, this most commonly relates to the health information of our beneficiaries.
Data Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The charity is the Data Controller for the personal data it processes.
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller. This includes any third-party contractors or service providers handling data under the charity's instruction.

These definitions underpin the practical procedures for conducting a DPIA, which are detailed in the following section.

5.0 Procedures

This section serves as the core operational guide for the policy, providing a practical, step-by-step methodology for embedding the DPIA process into the charity's project and operational lifecycle.

5.1 When to Conduct a DPIA

The charity must conduct a DPIA for any processing that is likely to result in a high risk to individuals. To determine if a full DPIA is required, a screening assessment must be completed at the start of any new project or change to existing processing.

A full DPIA is automatically mandatory if the processing involves any of the following:

1. Introduction of new technologies, systems, or software for processing personal data.
2. Processing of special category data (e.g., health data) or data on vulnerable individuals on a large scale.

3. Any proposed data processing that is likely to be perceived as intrusive by beneficiaries or goes beyond their reasonable expectations.
4. Processing that involves the systematic monitoring of individuals.
5. Any other processing that is identified as 'high risk' during the initial screening assessment.

5.2 The DPIA Process

When a full DPIA is required, the following six-step process must be followed and documented:

1. **Step 1: Identify the Need.** The project lead must complete an initial screening questionnaire to determine if the proposed processing is likely to result in a high risk. The Data Protection Officer (DPO) can provide guidance during this stage. If the screening indicates a high risk, a full DPIA is mandatory.
2. **Step 2: Describe the Processing.** The DPIA documentation must systematically describe the nature, scope, context, and purpose of the processing. This includes detailing the types of personal data involved, the source of the data, who will have access to it, and how it will be collected, used, stored, and deleted.
3. **Step 3: Assess Necessity and Proportionality.** This step evaluates whether the proposed processing is necessary to achieve the charity's legitimate objects, as stated in the charity's Constitution. The assessment must confirm that there is no less intrusive way to achieve the same outcome and that the processing is a proportionate response to the identified need.
4. **Step 4: Identify and Assess Risks.** Identify and assess the potential risks to the rights and freedoms of individuals. This must consider the potential impact of a data breach, unauthorised access, or other security failure, paying particular attention to the sensitivities of the Beneficiary Community. This includes considering the potential for distress or discrimination that could arise from a breach of data concerning health, wellbeing, or financial need, which are central to the charity's objects.
5. **Step 5: Identify Mitigating Measures.** For each risk identified in Step 4, identify and document the technical and organisational measures that will be put in place to reduce or eliminate that risk. This could include pseudonymisation, encryption, access controls, staff training, or revised procedures.
6. **Step 6: Sign-off and Record Outcomes.** The completed DPIA must be submitted to the DPO for review and advice. The DPO will advise on whether the remaining risks are acceptable. The final DPIA report, including all decisions and mitigating actions, must be formally signed off by the Board of Trustees. All DPIAs and their outcomes must be documented and retained.

Executing this process requires a clear understanding of who is responsible for each stage.

6.0 Roles and Responsibilities

The clear allocation of roles and responsibilities is fundamental to ensuring accountability and the successful implementation of the DPIA process throughout the charity.

- **Board of Trustees:** The Board of Trustees holds ultimate accountability for the charity's compliance with data protection law. This includes the non-delegable duties of ensuring this policy is implemented effectively, providing sufficient resources for its execution, and providing final scrutiny and sign-off for all DPIAs, particularly those with high residual risks.
- **Data Protection Officer (DPO):** Provides expert advice and guidance to Trustees and volunteers throughout the DPIA process. The DPO is responsible for reviewing completed DPIAs to assess compliance and advising on risk mitigation. The DPO's advice must be given independently and formally recorded. Where the DPO holds other roles within the charity (e.g., Trustee), particular care must be taken to manage any potential conflict of interest, and the independence of their DPO advice must be documented. The DPO is an appointed ordinary Trustee.
- **Trustees, Staff, and Volunteers:** All individuals managing projects or changing processes are responsible for identifying activities that may require a DPIA at the earliest stage. They are responsible for undertaking the screening assessment and, where required, conducting the full DPIA in consultation with the DPO and in line with this policy.
- **Contractors and Third-Party Suppliers:** Any external data processors are obligated under contract to cooperate fully and provide all necessary information to assist the charity in completing any DPIAs relevant to the services they provide.

These responsibilities form the foundation of the charity's plan for implementing this policy.

7.0 Implementation

A policy is only effective if it is properly implemented. This section outlines the practical steps the Board of Trustees will take to embed the DPIA policy into the charity's standard operating procedures and culture.

7.1 Timeline and Rollout

This policy is effective immediately upon its formal adoption by the Board of Trustees. It will be communicated to all Trustees, volunteers, and relevant third parties within 14 days of adoption.

7.2 Training

Mandatory awareness training on this policy and the practical application of the DPIA process will be provided to all Trustees within three months of the policy's adoption. This training will subsequently form a core component of the induction process for all new Trustees.

7.3 Resources

The Board of Trustees is responsible for ensuring that adequate resources, including time and access to DPO guidance and support, are allocated to enable individuals to carry out DPIAs effectively and without undue burden.

The effectiveness of this implementation will be tracked through a continuous monitoring and review cycle.

8.0 Monitoring, Review, and Audit

Ongoing monitoring and regular reviews are essential to ensure this policy remains effective, legally compliant, and fit for the charity's evolving purposes and operational activities.

The following mechanisms will be used for monitoring and review:

- **Key Performance Indicators (KPIs):** The number of DPIAs initiated and completed will be tracked as a measure of the policy's integration into project planning.
- **Reporting:** The DPO will provide a formal report to the Board of Trustees at least annually, summarising all DPIA activity, key risks identified, and the effectiveness of mitigating measures.
- **Review Schedule:** This policy will be formally reviewed by the Board of Trustees at least annually. An earlier review will be triggered by any significant changes to data protection legislation, ICO guidance, or the charity's data processing operations.
- **Audit:** Compliance with this policy and its associated procedures may be subject to periodic internal or external audit to provide independent assurance to the Board.

This DPIA policy operates within a wider framework of governance documents.

9.0 Related Policies and Documents

This Data Protection Impact Assessment Policy does not exist in isolation. It must be read and applied in conjunction with other key governance and policy documents to form a cohesive and comprehensive data protection framework.

Key related documents include:

- The charity's Constitution
- Data Protection Policy
- Information Security Policy
- Data Breach Notification Policy
- Subject Access Request (SAR) Policy
- Document Retention and Archiving Policy
- Risk Management Policy