International Data Transfer Policy

Document Control Table

Policy Title	**International Data Transfer Policy**
Document Reference	ORG/DP/013
Version	1.0
Effective Date	
Next Review Date	

1. Purpose and Legal Basis

As a charity entrusted with handling sensitive personal information for its beneficiaries, the charity has a profound legal and ethical duty to protect this data. This responsibility is paramount when information crosses national borders. This policy is not merely a procedural document; it is a strategic imperative designed to protect the charity's assets and reputation, manage regulatory risk, and secure the trust of the Beneficiary Community we serve.

The primary purpose of this policy is to establish a clear framework of rules and procedures to ensure that any transfer of personal data outside the United Kingdom is conducted lawfully, securely, and in a manner that protects the rights and freedoms of individuals.

Legal Framework

This policy is designed to ensure adherence to the key legislation governing data protection in the United Kingdom. All international data transfers undertaken by or on behalf of the charity must comply with:

- The UK General Data Protection Regulation (UK GDPR), with particular reference to the requirements outlined in Chapter 5.

- The Data Protection Act 2018.

This framework provides the legal foundation for the policy's scope and procedures.

2. Scope

A clearly defined scope is strategically important to ensure that all data processing activities are covered and that no compliance gaps exist. This policy applies universally to all processing of personal data undertaken by, or on behalf of, the charity.

Specifically, this policy applies to:

- All Charity Trustees, volunteers, and contractors acting on behalf of the charity.
- All personal and special category data is processed by the charity. This includes the particularly sensitive data relating to the beneficiaries from the "Beneficiary Community," as defined in the charity's constitution.
- All international data transfers, which include data being processed by third-party service providers (e.g., cloud storage platforms, communication tools, research partners) that are located outside of the UK or that may store data on servers outside the UK.

This scope ensures that everyone acting for the charity understands their obligations under this policy, which is founded upon the following core statement of intent.

3. Policy Statement

This statement serves as the foundational principle for all decisions regarding the international transfer of personal data. It represents the charity's core commitment to its beneficiaries, its partners, and its regulators, ensuring that the protection of personal data is a primary consideration in all operational activities.

The charity is absolutely committed to:

1. Not transferring personal data outside the United Kingdom unless robust, appropriate, and legally compliant safeguards are in place to protect that data.
2. Ensuring that the high level of protection afforded to personal data under UK law is not undermined by any international transfer.
3. Upholding the data protection rights of all individuals whose data we process, including trustees, volunteers, contractors, and, most importantly, our beneficiaries.

To implement this statement effectively, a common understanding of key terms is essential.

4. Definitions

Clear and consistent terminology is essential for the effective and accurate application of this policy. The following definitions are based on UK data protection law and are presented in the context of the charity's operations.

- **Personal Data**: Any information relating to an identifiable individual. This can include names, contact details, identification numbers, or any other information that can be used to identify a person directly or indirectly.
- **Special Category Data**: Sensitive personal data that requires a higher level of protection. This includes information about an individual's health, which is highly relevant to the charity's work with its beneficiary community.
- **International Data Transfer**: The act of sending personal data to, or making it accessible in, a country outside the United Kingdom. This includes, for example, using a US-based email marketing platform or storing beneficiary case files on a cloud server located in Ireland.
- **Restricted Transfer**: An international data transfer to a country that is not covered by a UK adequacy decision, meaning it requires additional safeguards.
- **Adequacy Decision**: A formal finding by the UK government that a specific country, territory, sector, or international organisation provides a level of data protection that is essentially equivalent to that in the UK.
- **Appropriate Safeguards**: Legally enforceable mechanisms that must be put in place for a restricted transfer to ensure data remains protected. The primary mechanism for the charity will be the UK's International Data Transfer Agreement (IDTA).
- **Transfer Risk Assessment (TRA)**: A mandatory assessment that must be conducted before a restricted transfer. It evaluates the specific risks of the transfer and confirms that the chosen appropriate safeguard (e.g., the IDTA) will provide effective protection in the legal and practical context of the destination country.
- **Beneficiaries**: As defined in Clause 3(1) of the charity's constitution.

These definitions underpin the procedures that must be followed for any international data transfer.

5. Procedures for International Data Transfers

A clear, step-by-step process is strategically necessary to ensure every international data transfer is lawful, secure, and properly documented. The following procedures are designed to guide trustees, volunteers, and contractors through a systematic evaluation before any transfer is initiated.

1. **Step 1: Identify the Transfer.** Before using a new service, system, or sharing data with a third party, you must first determine if the activity constitutes an international data transfer. This occurs if the data will be sent to, stored in, or be accessible from a country outside the UK. This includes using cloud services where servers are located abroad.

2. **Step 2: Check for an Adequacy Decision.** The first check is to verify if the UK Government has issued an "adequacy decision" for the destination country. The Information Commissioner's Office (ICO) maintains a current list of adequate countries. If an adequacy decision is in place for the destination country, the transfer can proceed without further safeguards. This decision must be documented.
3. **Step 3: Implement Appropriate Safeguards.** If no adequacy decision exists for the destination country, the transfer is a "restricted transfer" and must be protected by an 'appropriate safeguard'. For the charity, the primary safeguard to be used is the UK's International Data Transfer Agreement (IDTA). This is a legally binding contract that must be put in place with the data importer.
4. **Step 4: Conduct a Transfer Risk Assessment (TRA).** Alongside implementing an IDTA, a TRA is mandatory. The TRA must be conducted and documented to assess the specific risks of the transfer. It must evaluate the laws and practices of the destination country and confirm that the IDTA provides effective, enforceable protection for the data subjects in that specific context. If the risk is too high, the transfer cannot proceed.
5. **Step 5: Utilise Derogations (Exceptions)** In very rare and specific circumstances where neither an adequacy decision nor an appropriate safeguard is possible, a transfer may rely on a derogation. An example is gaining the data subject's explicit, informed consent for a specific transfer. Derogations are for exceptional, non-repetitive transfers only and require comprehensive justification and documentation. They must not be used for routine or systematic transfers.

Clear accountability is essential for the correct application of these procedures.

6. Roles and Responsibilities

Accountability is fundamental to effective data governance and risk management. This section clearly allocates responsibility for this policy's implementation, oversight, and day-to-day application across the charity's structure.

- **The Board of Trustees** holds ultimate responsibility for ensuring the charity complies with this policy and with all applicable data protection legislation. This includes formally adopting the policy, ensuring adequate resources are available for its implementation, and providing strategic oversight.
- **The Data Protection Officer (DPO)** is responsible for advising the Board on all aspects of this policy and its practical application. This includes providing guidance on conducting Transfer Risk Assessments, monitoring overall compliance with the policy, staying informed of changes in legislation, and acting as the primary point of contact for any data protection queries related to international transfers.
    - To ensure the independence of this role and to mitigate any potential conflicts of interest as required by UK GDPR, the charity must ensure that the DPO is not in a position that leads them to determine the purposes and

means of data processing. Where the DPO is also a Trustee, a formal conflict of interest assessment must be documented, and procedures put in place (e.g., recusal from certain decisions) to safeguard the role's independence.

- **Contractors and Volunteers** All contractors and volunteers are responsible for adhering to the procedures outlined in this policy during their day-to-day activities. They are required to identify potential international transfers and to inform the DPO before using any new system or sharing data with a third party that may involve transferring personal data outside the UK.

These roles work together to move the policy from a document to an active practice.

7. Implementation

A policy is only effective when it is properly embedded into the charity's operational culture. This section details the practical steps for the rollout, training, and resourcing of this policy to ensure its successful implementation.

- **Effective Date**: This policy is effective immediately upon its formal adoption by the Board of Trustees.
- **Training and Awareness** All trustees, volunteers, and key contractors must receive training on the requirements of this policy within three months of its adoption. This training will be refreshed periodically and will cover, at a minimum, how to identify a potential international transfer and the procedural steps that must be followed before any transfer can take place.
- **Resource Allocation** The charity will ensure that those responsible for implementing this policy have access to the necessary resources. This includes up-to-date guidance documents from the Information Commissioner's Office (ICO). The Board will also consider seeking specialist legal advice for any proposed transfer that is identified as being particularly high-risk or complex.

Successful implementation requires a commitment to ongoing oversight.

8. Monitoring and Review

This framework is designed to directly address the governance failings identified in the 2024 compliance review, where several key policies were found to be outdated. It establishes a clear and mandatory cycle of review and reporting to prevent recurrence.

Monitoring Mechanisms

The Data Protection Officer (DPO) will establish and maintain a central log of all approved international data transfers. This log will include copies of all completed Transfer Risk Assessments and the safeguards put in place, providing a clear audit trail of the charity's compliance activities.

Reporting

The DPO will provide a formal report to the Board of Trustees at least annually on all international data transfer activities undertaken by the charity. This report will highlight any risks or compliance issues identified during the period and recommend any necessary actions.

Policy Review

This policy will be formally reviewed by the Board of Trustees on an annual basis. A review will be conducted more frequently if there are significant changes to UK data protection legislation, new guidance from the ICO, or substantive changes to the charity's operations or data processing activities.

This policy operates as part of a wider suite of governance documents.

9. Related Policies and Documents

This policy operates as part of a wider, integrated governance framework. It should be read in conjunction with the following key documents, which are either in place or are scheduled for development as part of the charity's governance remediation programme recommended in its recent compliance review.

Related documents include:

- Data Protection Policy
- Information Security Policy
- Data Breach Notification Policy
- Subject Access Request Policy
- Document Retention Policy
- Third-Party Processor Due Diligence Procedure

Together, these documents form a critical part of the charity's commitment to good governance and the protection of those it serves.