# Data Breach Notification Policy

## Document Control

| Item | Detail |
|---|---|
| **Policy Title** | Data Breach Notification Policy |
| **Document Reference** | ORG/DP/001 |
| **Version** | 1.0 |
| **Effective Date** | |
| **Next Review Date** | |

---

## 1.0 Purpose and Legal Basis

Establishing a clear purpose and legal basis is foundational for any effective governance document. This section outlines the strategic importance of the Data Breach Notification Policy, anchoring it in both the charity's core mission and its legal obligations. A clear understanding of these foundations is essential for ensuring a response that is not only compliant with the law but also effective in protecting beneficiaries and maintaining the public's trust in the charity.

### 1.1 Purpose

This policy provides a critical framework for the charity's commitment to its beneficiaries and its regulatory duties. Its existence ensures a robust and transparent response plan is in place to protect the sensitive personal data entrusted to the charity by the Beneficiary Community, as any breach could cause significant harm to beneficiaries and inflict lasting reputational damage. The two core objectives of this policy are:

- To provide a clear, systematic, and timely procedure for identifying, investigating, and responding to any suspected or actual personal data breach.
- To ensure the charity meets its legal and regulatory obligations under UK data protection law.

### 1.2 Legal Basis

This policy is established under the following legal and regulatory framework:

- UK General Data Protection Regulation (UK GDPR), specifically Articles 33 and 34 concerning the notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject.
- Data Protection Act 2018 (DPA 2018), which supplements and is to be read in conjunction with the UK GDPR.
- The Data (Use and Access) Act 2025, which the charity acknowledges as a forward-looking compliance consideration for data governance.
- Charity Commission guidance on good governance, accountability, and the responsibilities of trustees in safeguarding charitable assets, including personal data.

This policy applies comprehensively across the charity's operations, as detailed in the following section.

---

## 2.0 Scope

A clearly defined scope is strategically vital, as it ensures that the policy is applied universally and consistently across the organisation. This section clarifies precisely who and what is covered by these procedures, leaving no ambiguity in its application and guaranteeing that all individuals and data assets receive the same high standard of protection.

### 2.1 Individuals Covered

- All individuals acting on behalf of the charity, including Trustees, any future employees, volunteers, and third-party contractors or service providers who have access to the charity's personal data.

### 2.2 Activities/Data Covered

- All personal data created, collected, stored, or processed by the charity, regardless of its format (including electronic records, paper files, and other media).

This unified approach reflects the Board of Trustees' formal commitment to data security.

---

## 3.0 Policy Statement

A formal policy statement serves as the definitive declaration of intent from the Board of Trustees. It establishes the standard for the charity's commitment to data security and sets the tone for the entire organisation, reinforcing the principle that protecting personal information is a fundamental responsibility.

The Board of Trustees of the charity is steadfastly committed to:

- Protecting the confidentiality, integrity, and availability of the personal data entrusted to it, particularly the sensitive information of its beneficiaries.
- Implementing and maintaining effective procedures to detect, report, and thoroughly investigate any suspected or actual personal data breach.
- Responding to any data breach in a timely, lawful, and transparent manner to mitigate any potential harm to individuals.
- Fostering a culture of transparency and data security awareness among all trustees, volunteers, and partners to ensure that data protection is a shared responsibility.

To implement this policy effectively, it is essential that all parties understand the key terms that underpin it.

---

## 4.0 Definitions

Clear definitions are essential for the consistent and correct application of this policy. A shared understanding of key terms is vital for ensuring that all trustees and volunteers can act confidently and correctly, removing ambiguity and supporting a uniform response in the event of an incident.

| Term | Definition |
| --- | --- |
| **Personal Data Breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples relevant to the charity include: sending an email containing sensitive beneficiary information to the wrong recipient; the loss or theft of an unencrypted laptop holding grant application details; or unauthorised access to the charity's database by a malicious third party. |

| | |
|---|---|
| **Personal Data** | Any information relating to an identified or identifiable living individual. Examples specific to the charity include: names, contact details, and personal histories of beneficiaries, their families, and descendants; and the personal information of trustees and volunteers. |
| **Data Controller** | The organisation that determines the purposes and means of processing personal data. For the purposes of this policy, **the charity** is the Data Controller. |
| **Data Processor** | A third-party organisation or individual that processes personal data on behalf of the Data Controller. This may include contractors engaged by the charity to manage IT systems, communications, or other services. |
| **Information Commissioner's Office (ICO)** | The UK's independent supervisory authority responsible for enforcing data protection law. |

These definitions form the basis for the operational procedures that must be followed in the event of a data breach.

---

## 5.0 Procedures

These procedures form the core, step-by-step operational guide for responding to a data breach. They are designed to ensure a swift, compliant, and effective response that protects the charity's beneficiaries, mitigates risk, and meets all regulatory duties in a structured and auditable manner.

### 5.1 Breach Identification and Internal Reporting

Any Trustee, volunteer, or contractor who discovers or suspects that a personal data breach has occurred must take immediate action. All suspected breaches, no matter how minor they may seem, must be reported immediately to the designated Data Protection Officer (DPO). The initial report should include as much detail as is available about the nature of the incident.

### 5.2 Containment and Recovery

Upon receiving a report, the DPO must take immediate steps to contain the breach and limit its impact. The primary goal of this phase is to recover control and prevent any further unauthorised access to or loss of data. Containment actions may include, but are not limited to:

- Isolating an affected IT system from the network.
- Instruct a recipient to delete an email sent in error.
- Changing access passwords and credentials for compromised accounts.
- Remotely wiping a lost or stolen device.

### 5.3 Risk Assessment

The DPO must promptly conduct a risk assessment to understand the severity of the breach and the potential risk to the rights and freedoms of the individuals whose data is affected. This assessment must consider factors such as:

- The type and volume of personal data involved.
- The sensitivity of the data, paying special attention to the vulnerability of the charity's beneficiary community.
- The likelihood and severity of potential harm to individuals, including emotional distress, financial loss, or other significant impacts.

### 5.4 Notification to the Information Commissioner's Office (ICO)

If the risk assessment concludes that the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO must report it to the ICO without undue delay, and not later than 72 hours after the charity becomes aware of it. The notification must contain:

- A description of the nature of the personal data breach.
- The categories and approximate number of individuals and personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the breach.
- A description of the measures taken or proposed to be taken to address the breach.

### 5.5 Notification to Affected Individuals

If the risk assessment concludes that the breach is likely to result in a high risk to the rights and freedoms of individuals, the charity must communicate the breach to the affected individuals directly and without undue delay. This communication must be in clear and plain language, demonstrating sensitivity and respect for the beneficiary community. It must include the nature of the breach, its likely consequences, the measures being taken to mitigate harm, and advice on how individuals can protect themselves.

### 5.6 Post-Breach Review and Record Keeping

Following any breach, the DPO will lead a review to identify the cause of the incident and determine what lessons can be learned. The findings will be used to implement improvements to systems, policies, and training to prevent a recurrence. The charity must maintain an internal register of all data breaches, including those not reported to the ICO, to document the facts, effects, and remedial actions taken.

Executing these procedures effectively relies on clearly defined roles and responsibilities.

---

## 6.0 Roles and Responsibilities

Clearly defined roles and responsibilities are vital for the effective execution of the breach response plan. Accountability is the cornerstone of good governance, ensuring that every individual understands their specific duties and that the entire response process is managed with precision and authority.

Clear accountability is vital for the effective implementation and execution of this data breach response policy. While the Data Protection Officer (DPO) role is currently assigned to an ordinary Trustee appointed by the Board of Trustees, the Board of Trustees acknowledges its responsibility to manage any potential conflicts of interest inherent in this dual-role arrangement, in line with good governance principles. The following table outlines the key responsibilities assigned to specific roles within the charity.

| Role | Assigned Responsibilities |
|---|---|
| **Board of Trustees** | Holds overall accountability for the charity's data protection compliance.<br><br>Ensures that adequate resources are available for effective breach management.<br><br>Receives and reviews reports on data breaches and lessons learned from the DPO. |
| **Data Protection Officer (DPO)** | - Acts as the single point of contact and lead for managing the breach response process<br><br>- Leads the containment, recovery, and risk assessment procedures. |

| | |
|---|---|
| | - Handles all mandatory notifications to the ICO and affected individuals.<br><br>- Maintains the internal data breach register.<br><br>- Provides guidance and support to trustees and volunteers on data protection matters. |
| **All Trustees, Volunteers, and Contractors** | Have a mandatory duty to report any suspected data breach immediately to the DPO.<br><br>Must cooperate fully with any subsequent investigation into a data breach. |

These responsibilities will be embedded into the charity's operations through a structured implementation plan.

---

## 7.0 Implementation

An implementation plan is strategically important as it outlines the practical steps the Board will take to move this policy from a document to an active part of the charity's culture. This section ensures the policy is properly adopted, communicated, and resourced, embedding it into the organisation's operational framework.

1. **Adoption:** This policy will be formally adopted by a resolution of the Board of Trustees and its effective date recorded.
2. **Communication:** The adopted policy will be communicated to all Trustees, volunteers, and relevant third-party contractors to ensure they are aware of its contents and their obligations.
3. **Training:** All Trustees and volunteers will receive mandatory training on this policy and their specific data breach reporting responsibilities. This training will form a core part of the induction process for all new Trustees and volunteers.
4. **Resources:** The DPO will be provided with the necessary resources to manage a data breach effectively, including access to up-to-date ICO guidance, reporting templates, and support channels.

The ongoing effectiveness of this policy will be ensured through a regular monitoring process.

---

## 8.0 Monitoring, Review, and Reporting

Ongoing monitoring is essential to ensure that this policy remains effective, compliant with legal requirements, and fit for purpose over time. This process of continuous oversight provides assurance to the Board and stakeholders that the charity's data breach response capability remains robust and relevant.

- **Key Performance Indicators (KPIs):** The internal data breach register will be reviewed quarterly by the DPO to track the number and nature of incidents, identify any trends or systemic issues, and assess the effectiveness of remedial actions.
- **Reporting:** The DPO will provide a formal report to the Board of Trustees at least annually on any data breaches that have occurred, the actions taken, and the lessons learned.
- **Review Schedule:** This policy will be formally reviewed by the Board of Trustees at least annually, or more frequently if there are significant changes to data protection legislation, the charity's operations, or following a major data breach.

This policy should be read and applied in conjunction with other key governance documents.

---

## 9.0 Related Policies and Documents

Understanding how this policy interrelates with other governance documents is crucial for a cohesive and comprehensive approach to risk management. This policy operates as part of a wider suite of documents that collectively protect the charity, its beneficiaries, and its stakeholders.

- Data Protection Policy
- Information Security Policy
- Subject Access Request (SAR) Policy
- Document Retention and Archiving Policy
- Complaints Handling Policy
- Risk Management Policy