# Information Security Policy for the charity

## 1.0 Document Control Table

Formal document control is a critical governance discipline, providing the auditable framework essential for maintaining the trust of the beneficiary community and protecting their highly sensitive personal data. It ensures that the charity's policies remain relevant, compliant with current legislation, and consistently applied across all operations, providing a clear structure for accountability, review, and continuous improvement.

| | |
|---|---|
| **Policy Title** | **Information Security Policy** |
| **Document Reference** | ORG/DP/006 |
| **Version** | 1.0 |
| **Effective Date** | |
| **Next Review Date** | |

This policy outlines the charity's mandate and procedures for securing its information assets against internal and external threats.

## 2.0 Purpose and Legal Basis

A clear and robust Information Security Policy is a cornerstone of the charity's governance, essential for upholding the profound trust placed in it by the Beneficiary Community. Its strategic importance lies in its role in protecting their highly sensitive personal and health information. By establishing robust security measures, this policy safeguards the charity's reputation, its assets, and its ability to fulfil its charitable mission.

The core purposes of this policy are:

- To establish a coherent framework of technical and organisational measures to protect all of the charity's information assets from security threats.
- To define clear roles and responsibilities for the management and oversight of information security across the charity.
- To ensure the confidentiality, integrity, and availability of information processed by trustees, volunteers, and third-party contractors.
- To mitigate risks of data breaches and ensure a swift, compliant response should an incident occur, address gaps identified through governance compliance reviews.

**Legal Basis**

This policy is designed to ensure the charity's compliance with its legal and regulatory obligations. All activities undertaken in relation to this policy must adhere to the following key legislation and guidance:

- The UK General Data Protection Regulation (UK GDPR), particularly the security principle under Article 32.
- The Data Protection Act 2018.
- The Equality Act 2010, in relation to protecting the data of all individuals without discrimination.
- The Data (Use and Access) Act 2025, regarding principles of data re-use.
- Guidance from the Charity Commission for England and Wales on good governance and the protection of charity assets.

The principles and procedures outlined herein apply to all individuals who handle the charity's information and to all data assets under its control, as defined in the following section.

## 3.0 Scope

A comprehensive scope is essential for ensuring that all individuals handling beneficiary data and all sensitive information assets, from health information to governance records, are protected by consistent security standards, leaving no gaps in the charity's protective measures. This policy is comprehensive in its reach, applying to all individuals who have authorised access to the charity's information assets and to all information critical to its operations, regardless of its format (digital or physical) or location.

**Application**

This policy applies to all individuals and groups who access, process, or manage information on behalf of the charity, including:

- Charity Trustees
- Staff (if any are appointed)
- Volunteers and Associate Members

- External contractors and third-party service providers who process data on behalf of the charity.

**Information Assets**

This policy protects all of the charity's information assets, with particular emphasis on the sensitive data it handles to fulfil its objects. This includes, but is not limited to:

- **Beneficiary Data:** All personal and special category data relating to the Beneficiary Community, including grant applications, health information, communications, and heritage materials.
- **Financial Data:** Information relating to the charity's investments, financial controls, grant making activities, and banking.
- **Governance and Operational Data:** Minutes of trustee meetings, strategic plans, internal communications, and contractor agreements.

The charity is formally committed to protecting all individuals and information assets that fall within the scope of this policy, a commitment articulated in the formal policy statement.

## 4.0 Policy Statement

The policy statement is the formal, high-level commitment from the Board of Trustees. It establishes the standard for the entire organisation's approach to protecting the sensitive health and personal data of the Beneficiary Community.

The Board of Trustees of the charity formally affirms its unwavering commitment to protecting the confidentiality, integrity, and availability of all its information assets. The Board is committed to upholding the profound trust placed in it by our beneficiaries by handling their personal and sensitive information with the utmost care and respect. We are committed to complying with all relevant UK data protection and charity law and to fostering a culture of security awareness among all trustees, volunteers, and partners.

To ensure a shared understanding of this commitment, a clear definition of key terms is required.

## 5.0 Definitions

Clear, consistent terminology is vital for the effective implementation of this policy, ensuring all trustees, volunteers, and partners have a shared understanding of key concepts, which is vital when handling the sensitive personal and health data of our beneficiaries.

| Term | Definition |
| --- | --- |
| Information Assets | Data, information, and the systems that store or process it. For the charity, this includes beneficiary databases, financial records, grant applications, meeting minutes, and email systems. |
| Personal Data | Any information relating to an identifiable individual, such as a name, address, or email, as defined by UK GDPR. |
| Special Category Data | Sensitive personal data that requires a higher level of protection. For the charity, this primarily includes health information that may be processed in relation to its beneficiaries. |
| Confidentiality | The principle of ensuring that information is accessible only to those with authorised access. |
| Integrity | The principle of safeguarding the accuracy and completeness of information and the methods used to process it. |
| Availability | The principle of ensuring that authorised users have access to information and associated assets when required to perform their roles. |
| Information Security Incident | A single or series of unwanted or unexpected information security events that have a significant probability of compromising charity operations and threatening information security. |
| Data Breach | An information security incident that has resulted in the confirmed accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. |

These definitions provide the foundation for the detailed operational procedures that follow.

## 6.0 Procedures

This section provides the mandatory, practical, and detailed steps required to implement the policy's principles. These procedures establish the baseline of security controls designed to protect the charity's information assets, particularly the sensitive data of the Beneficiary  Community.

1. **Access Control**
    - Access to the charity's data and systems must be managed based on the principle of 'least privilege', meaning individuals are only granted access to the information necessary to perform their specific role.
    - Access rights for all trustees, volunteers, and contractors must be formally reviewed at least annually and immediately upon a change in their role or their departure from the charity.
    - All individuals accessing charity systems must use strong, unique passwords (or passphrases) and must not share their login credentials.
2. **Data Handling** Mandatory security measures must be applied to data at all stages of its lifecycle.
    - **Data Storage:** All sensitive personal and special category data stored digitally must be encrypted. Physical records containing such data must be stored in secure, lockable filing cabinets or rooms with restricted access.
    - **Data Transmission:** Any transmission of sensitive or confidential data via email or other electronic means must be encrypted and protected to prevent interception.
    - **Data Disposal:** Information assets must be disposed of securely when no longer required, in line with the charity's Document Retention and Archiving Policy. This requires shredding for physical documents containing personal or confidential information and secure, irreversible deletion for digital files.
3. **Physical Security** Physical security measures must be implemented to secure any location where charity information is stored or processed. This includes securing office spaces and ensuring that sensitive beneficiary records and financial documents are stored in locked cabinets.
4. **Third-Party and Contractor Security**
    - A formal due diligence process must be conducted before engaging any new contractor that will process charity data. This process must rigorously assess their compliance with UK GDPR and the adequacy of their technical security measures, replacing any previous inadequate questionnaires.
    - All contractor agreements must include specific data protection clauses that legally bind them to meet or exceed the standards set out in this policy and to report any security incidents without delay.

5. **Information Security Incident and Data Breach Management:** A clear, step-by-step procedure is required in the event of a suspected information security incident.
    - **Step 1: Reporting:** Anyone who suspects an incident has occurred must immediately report it to the designated lead (e.g., the Data Protection Officer).
    - **Step 2: Assessment:** The designated lead must promptly assess the incident to determine its nature, severity, and whether a personal data breach has occurred.
    - **Step 3: Containment and Recovery:** Immediate action must be taken to contain the incident, limit the damage, and begin the process of recovering affected systems or data.
    - **Step 4: Notification:** The charity is committed to reporting personal data breaches to the Information Commissioner's Office (ICO) and affected individuals where legally required. This process is governed by the charity's separate Data Breach Notification Policy.

For these procedures to be effective, their implementation relies on clearly assigned roles and responsibilities.

## 7.0 Roles and Responsibilities

Clear accountability is essential for effective information security, particularly when protecting the sensitive data of a vulnerable beneficiary community. This section assigns specific responsibilities across the organisation to ensure this policy is implemented and maintained consistently.

| **Role** | **Specific Responsibilities** |
|---|---|
| The Board of Trustees | Holds ultimate responsibility for the charity's information security. The Board is responsible for formally approving this policy, ensuring adequate resources are available for its implementation, and promoting a culture of security awareness. |
| Data Protection Officer (DPO) / Designated Lead | Overseeing the day-to-day implementation of this policy. Acting as the primary point of contact for security incidents. Leading due diligence for third parties. Providing guidance and training to trustees and volunteers. |

| | |
|---|---|
| | This role will be an ordinary Trustee, appointed by the Board of Trustees.<br><br>Note: This role must be structured to mitigate the conflict of interest risk identified in the governance review, ensuring the post-holder has sufficient operational independence from the Board's decision-making on data processing activities. |
| All Trustees, Staff, and Volunteers | Responsible for understanding and complying with this policy in their daily activities. This includes using the charity's information assets responsibly and promptly reporting any suspected security incidents to the designated lead. |
| Contractors and Third Parties | Responsible for complying with the information security standards set out in their contracts and for immediately reporting any security incidents involving charity data to their designated charity contact. |

These defined roles are central to the plan for embedding the policy into the charity's operations.

## 8.0 Implementation

A policy is only effective when it is properly communicated and embedded into the charity's culture, ensuring that protecting beneficiary information becomes a shared responsibility for all trustees and volunteers. This section details the plan for achieving this.

To ensure this policy is embedded effectively, the Board has approved the following implementation plan:

1. **Communication:** This policy will be formally communicated to all individuals within its scope, including all trustees, volunteers, and key contractors, to ensure they are aware of their responsibilities.
2. **Training and Awareness:** Initial awareness training on the key principles of this policy and their practical application will be provided to all trustees and volunteers. This training must be refreshed at least annually to maintain awareness of current threats and best practices.
3. **Resource Allocation:** The Board of Trustees is responsible for allocating any necessary resources (e.g., for secure software, specialist training, or expert advice) to support the effective implementation of this policy.

4. **Timeline:** This policy will be fully communicated and initial awareness training completed within three months of the effective date.

Once implemented, the policy's effectiveness must be continuously monitored to ensure it remains fit for purpose.

## 9.0 Monitoring, Review, and Audit

Given the dynamic nature of information security threats and the sensitive health data the charity processes, ongoing monitoring is a critical governance function. This section establishes the framework for ensuring the policy remains effective, relevant, and compliant over time.

### Monitoring Mechanisms

The DPO/Designated Lead will monitor the implementation of this policy and will report on any security incidents and the overall state of information security to the Board of Trustees at their regular meetings.

### Review Schedule

This policy will be formally reviewed by the Board of Trustees at least annually. A review will also be triggered by any significant changes to legislation, the charity's operations, or in response to a major security incident.

### Key Performance Indicators (KPIs)

The following indicators will be used to measure the policy's effectiveness:

- Number of security incidents reported and resolved.
- Percentage of trustees and volunteers who have completed annual security awareness training.
- Timely completion of the annual policy review.

This policy forms part of a wider network of documents that collectively define the charity's approach to governance.

## 10.0 Related Policies and Documents

Information security does not exist in isolation but is part of an integrated governance framework. This policy should be read in conjunction with other key governance documents to ensure a comprehensive and integrated approach to managing risks to the charity and its beneficiaries.

The following documents are directly related to this policy:

- Data Protection Policy

- Data Breach Notification Policy
- Document Retention and Archiving Policy
- Conflict of Interest Policy
- Internal Financial Controls Policy
- Risk Management Policy