Data Protection and Management Policy

Introduction

Introduction and Scope

This policy outlines our trust's commitment to data protection and compliance with the UK Data Protection Act. Its purpose is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on our behalf, including trustees, staff, and volunteers.

Data Protection Lead

We will appoint a Data Protection Lead who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities.

Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is a UK law that regulates the processing of personal data. The UK Information Commissioner's Office (ICO) provides guidelines on data protection that we follow.

UK GDPR: The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
Data Processor: An individual or organisation that processes personal data on behalf of a data controller.
Data Controller: An individual or organisation that determines how and why personal data is processed.
Data Subject: An individual whose personal data is being processed.
Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.
Personal Data: Any information that can identify a living individual, such as name, address, or email address.

Sensitive Personal Data: Personal data that requires extra protection, such as health information or ethnic origin.
Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.
PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.
Valid Consent: Consent given freely, specifically, and informed, and can be withdrawn at any time.
Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

Data Protection Principles

Data is:

- **Processed lawfully, fairly and in a transparent manner.**
    - There are several grounds on which data may be collected, including consent.
    - We are clear that our collection of data is legitimate and we have obtained consent to hold an individual's data, where appropriate.
    - We are open and honest about how and why we collect data and individuals have a right to access their data.
- **Collected for specified, explicit and legitimate purposes and not used for any other purpose.**
    - We are clear on what data we will collect and the purpose for which it will be used.
    - And only collect data that we need.
    - When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.
- **Adequate, relevant and limited to what is necessary.**
    - We collect all the data we need to get the job done.
    - And none that we don't need.
- **Accurate and, where necessary, kept up to date.**
    - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.
    - We correct any mistakes promptly.
- **Kept for no longer than is necessary**. We understand what data we need to retain, for how long and why.
    - We only hold data only for as long as we need to.
    - That includes both hard copy and electronic data.
    - Some data must be kept for specific periods of time (eg accounting, H&SW).
    - We have some form of archive/review policy/process that ensures data no longer needed is destroyed.
- **Processed to ensure** appropriate security, not only to protect against unlawful use, but also loss or damage. We follow the ICO guidance on data storage, sharing and security.

- **Data is held securely**, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected.
- **Data is kept safe.** Our IT systems have adequate anti-virus and firewall protection that's up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
- **Data is recoverable.** We have adequate data back-up and disaster recovery processes.

Privacy Notices

A privacy notice tells people what you do with their personal data and is a key part of being open and transparent. We provide clear, simple and accessible privacy notices whenever we collect personal data, for example on forms, websites or sign-up processes. These explain what data we collect, why we need it, how we use it, who we share it with, how long we keep it, and the rights individuals have. We make sure our privacy information is easy to understand and keep it up to date.

ICO: Privacy notice generator (toolkit).

Individual Rights

We recognise that individuals' rights include the right to be informed, of access, to rectification, erasure, restrict processing, data portability and to object.

Use of Imagery/Video

All imagery is protected by copyright and cannot be used without the consent of the owner, usually the person who took the image. You may also need consent from the individuals in images of individuals and small groups, which may well fall within the Data Protection Act. However, there is some ambiguity, so err on the side of caution and obtain consent wherever this is reasonably possible. Particular care is to be taken when using images of children or other vulnerable people. Here are some questions to consider when using imagery:

- For what purpose was the original image taken? If it was for one purpose, such as personal use, it cannot be used for another without the consent of the individuals concerned
- Is the image sensitive personal data? If it is, do you have the individual's consent?
- For small groups and individuals, has an image consent form been used?
- When using images of children, or people who may not be competent, do you have valid consent?
- When using images of children or other vulnerable people, are you confident your use of the image will not place them at risk? Particularly, if it is to be used publicly, such as in the Media or on the web.
- When photographing large groups, have the individuals been given a chance to opt out of the photograph?
- Has the person/people in the image been told how the image will be used?
- Are you using the image according to how the person/people were told it would be used?

Recording Devices

Smart glasses, wearable devices, mobile phones, or any other device that can take photos, record video, record sound, or create AI transcripts may only be used if:

- Those present have given their informed consent and;
- The purpose, storage and retention of recordings meet fully the charity's data protection requirements.

Such devices must not be used:

- During safeguarding, casework, counselling, health, financial, HR or other confidential activities except where expressly authorised.
- To record children or vulnerable adults.

Information Commissioner's Office (ICO):

- Video Surveillance Guidance.
- Data Protection Principles for Surveillance Systems.

Recording Devices

Smart glasses, wearable devices, mobile phones, or any other device that can take photos, record video, record sound, or create AI transcripts may only be used if:

- Those present have given their informed consent and;
- The purpose, storage and retention of recordings meet fully the charity's data protection requirements.

Such devices must not be used:

- During safeguarding, casework, counselling, health, financial, HR or other confidential activities except where expressly authorised.
- To record children or vulnerable adults.

Data Breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
We will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where there will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence.
We will notify the ICO within 72 hours, of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- Result in discrimination.
- Damage to reputation.
- Financial loss.
- Loss of confidentiality or any other significant economic or social disadvantage.

Complaints

In line with the ICO's guidance and the Data (Use and Access) Act 2025, we have a dedicated process for handling complaints relating to personal data. Anyone who believes we have not handled their personal information appropriately may raise a data protection complaint with us.

We will:

- Provide a clear and accessible way for individuals to submit data protection complaints.
- Acknowledge receipt of such complaints within 30 calendar days.
- Take appropriate steps to investigate the complaint without undue delay, including making necessary enquiries and keeping the complainant informed throughout.
- Communicate the outcome of the complaint promptly and clearly, explaining any actions taken or decisions made.

All complaints will be handled fairly, transparently, and in accordance with our obligations under the Data Protection Act. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner's Office (ICO).

Fundraising

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors.

The ICO's "charitable purpose soft opt-in" allows us to send fundraising emails, texts, and similar messages without explicit consent, but only in tightly defined circumstances. In practice, we can rely on it where someone has actively engaged with our charity – for example by donating, volunteering, or expressing clear interest in our work – and we collected their contact details directly at that point. The communication must be solely about our own charitable purposes (such as fundraising appeals, campaigns, or volunteering), and not about other organisations or commercial activity.

To use this lawfully and safely, we will build compliance into how we collect and use data. We will give individuals a clear and simple opportunity to opt out when we first collect their details, and we will repeat that opt-out option in every message we send. We will not use contact details obtained from third parties, including fundraising platforms or purchased lists. The rule applies only to data collected from 5 February 2026 onwards and is not retrospective. In practice, this means we may need to operate parallel approaches: consent-based marketing for older contacts and soft opt-in for new supporters, while ensuring we do not stretch what constitutes genuine "supporter interest" or risk breaching PECR.

More detailed information has been issued by the Regulators.

- **Information Commissioner's Office (ICO):** Charities given new flexibility to contact supporters under data law change.
- **Fundraising Regulator:**
  - Charitable purposes soft opt-in and fundraising marketing.
  - Data Privacy and Fundraising.

And Bates Wells LLP have issued their own practical plain English interpretation of that.

- **BWB:** ICO publishes guidance on use of the 'charity soft opt-in'.

Fundraising Preference Service

We will respect the privacy and contact preferences of our donors. We will respond promptly to requests to cease contacts or complaints and act to address their causes.

Artificial Intelligence

We have adopted and comply with the Charity AI Ethics & Governance Framework and ICO AI guidance. If AI is used to allow access to data sets containing personal information, such as staff or beneficiary records, we have carried out an AI Risk Analysis and a data protection impact assessment (DPIA) and updated our data protection policy and procedures to reflect this.

Data Retention

Our data will only be kept for as long as there is an administrative need to do so in order to enable our charity to carry out its business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or to meet legislative requirements.

In general, records are kept for 6 years after the end of the accounting year to which they relate but we do not keep personal records any longer than necessary and certain records may be required to be retained for longer. Factors affecting retention periods include legal requirements, storage costs, historical value, industry standards, and archival needs.

Subject Access Requests

A Subject Access Request (SAR) is when someone asks to see the personal data you hold about them. We make this as easy as possible for people and will respond within one month, as required by law. We check the identity of the person making the request, gather the relevant information, and provide it clearly and securely. If a request is complex, we may extend the deadline in line with ICO rules and will explain this to the individual.

Data Sharing

We only share personal data where there is a clear lawful reason to do so, such as delivering services, meeting legal requirements, or working with trusted partners. Before sharing, we check that it is necessary and proportionate, and that appropriate safeguards are in place. We never share data for unrelated purposes and always respect individuals' rights and expectations.

Third Party Processors

If we use external organisations (such as IT providers, CRM systems, or payroll services) to process data on our behalf, we will make sure these organisations only act on our instructions and have appropriate contracts in place to protect personal data. We also carry out basic checks to ensure they have suitable security and data protection standards.

Records of Processing (ROPA)

We keep clear records of what personal data we hold, where it comes from, how it is used, and who it is shared with. This helps us stay organised, demonstrate compliance, and respond quickly to requests or issues.

Version Control - Approval and Review

This policy will be reviewed periodically, or following an incident, change in legislation, or other significant factors.

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	October 26	Initial policy	Annually

Regulatory Guidance

ICO: UK GDPR guidance and resources. A whole range of resources.