Data Protection Policy

beyond food
inspiring a future
beyond homelessness

Applicability

This policy applies to all members of our charity, including trustees. Therefore, everyone must follow this policy in respect of compiling data.

The Data Protection Act is complex, but is based on respecting peoples' wishes and only using their personal data, in a way that they would wish us to. Something that we all want for ourselves and that is particularly important when working with vulnerable people.

This policy has been kept short and simple, to make it as accessible as possible to everyone. As such, it cannot be definitive and other policies may be issued to cover specialist areas, if necessary. It covers the fundamental, practical application of the Data Protect Act that is to be complied with by anyone in our organisation who manages or has responsibility for personal data.

Data protection principles

Data is:

1. 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.
2. 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.
3. 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.
4. 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.
5. 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 ensure data no longer needed is destroyed.

6. Processed to ensure Appropriate security, not only to protect against unlawful use, but also loss or damage.
    - 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.

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.

Special category (sensitive) data needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation. Due diligence should be taken to safeguard this information.

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. We will also secure the consent from the individuals in images of individuals and small groups, which also fall within the Data Protection Act. Particular care will be taken when using images of children or other vulnerable people. People under 13 years of age are not legally able to give consent.

Some people are unable, or may be unable to give consent, and this must be obtained from the person who is able to make decisions on their behalf, such as a Lasting Power of Attorney. Any decisions that you may make on their behalf, must always be in their best interests.

Due diligence 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?

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.

Responsibilities

Trustees. Ultimately the Board of Trustees is responsible for data protection. A committee or lead trustee may be delegated the responsibility for data protection, periodic review of the policy and any breaches must be maintained.

Executive. Trustees may formally appoint a Data Protection Officer (CEO), but someone should be made specifically responsible for leading on data protection.

Specialist. Trustees/CEO may nominate individuals to take responsibility for areas linked to data protection, where particular data protection expertise is required. For example, IT or fundraising.

Help And Support

When required we will seek help and support from the regulator, the Information Commissioner's Office (ICO) [a link to guidance for charities here], or to contact the ICO by phone, e mail or live chat, [link here]. A self-assessment tool and other resource links are available [link here].

Approval and Review

Approval By	Date	Next Review Date
Trustee Board	January 2021	January 2022