

Brighter Together

Connecting the old and young to shine brighter together

GDPR Policy

Endorsement Date	11/09/2020
Next Review Date	11/09/2021
Overall Responsibility for Policy	Trustees
Responsibility for Policy Implementation	Andrew Melia (Chair of Trustees)
Audience	All volunteers, staff, consultants, advisors & trustees
Relevant Legislation & Statutory Guidance	Data Protection Act 2018

Brighter Together

Connecting the old and young to shine brighter together

Purpose

This policy sets out how we seek to protect personal data and ensure that staff and volunteers understand the principles governing their use of personal data to which they have access in the course of their work. It also sets out how we seek to comply with General Data Protection Regulations (GDPR).

Definitions

Charity	means Brighter Together, a registered charity (1190557).
GDPR	means the General Data Protection Regulation.
Responsible Person	means Polly van Marken.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.
Controller	A controller determines the purposes and means of processing personal data.
Processor	A processor is responsible for processing personal data on behalf of a controller.
Personal Data	Personal data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Scope

This policy applies to all staff and volunteers involved in processing data. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email

Brighter Together

Connecting the old and young to shine brighter together

use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Data Protection Principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

General provisions

- a. This policy applies to all personal data processed by the Charity.
- b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.

Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
- b. The Register of Systems shall be kept up to date on an ongoing basis for any new data requirements the Charity has. This will be maintained by the Responsible Person.

Brighter Together

Connecting the old and young to shine brighter together

- c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt within one month.

Lawful purposes

- a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).
- b. The Charity shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

Data minimisation

- a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- a. The Charity shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

Security

- a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up to date. It is the responsibility of staff members and volunteers who have access to data to ensure that their computers are up to date with windows updates, and antivirus software and that their mobile devices are encrypted.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be in place.

Brighter Together

Connecting the old and young to shine brighter together

Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

When a personal data breach has occurred, we will:

- Try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.
- Establish the likelihood and severity of the resulting risk to people's rights and freedoms.
- If it is likely that there will be a risk then we must notify the ICO without undue delay and within 72 hours of becoming aware of it, telling them:
 - a description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned.
 - the categories and approximate number of personal data records concerned.
 - the name and contact details of the Responsible Person where more information can be obtained.
 - a description of the likely consequences of the personal data breach.
 - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.
- We must inform those concerned directly as soon as possible
- We will record all breaches, regardless of whether they need to be reported to the ICO, including:
 - the facts relating to the breach,
 - its effects
 - the remedial action taken.

We will investigate whether the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training, or other corrective steps.

Accountability and Governance

- a. Our Data Protection Policy and Register of Systems will be reviewed annually and agreed by Trustees.
- b. All staff will receive compulsory training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Brighter Together

Connecting the old and young to shine brighter together

Signature

This policy statement came into force on

We are committed to reviewing our policy and good practice annually. This policy statement and accompanying procedures were last reviewed

Signed by: Andrew Melia (on behalf of all Brighter Together Trustees)



.....

Job Title: Chair of Trustees, Brighter Together

Date: 11th Sept 2020

Signed by: Polly van Marken

.....

Job Title: Founder, Brighter Together

Date: 11th Sept 2020