Brighter Together

Creating connections that light up lives

Data Protection Policy

Endorsement Date	09/03/2026
Next Review Date	09/03/2028
Policy Owner	Board of Trustees
Responsibility for Policy Implementation	Chief Executive
Audience	All employees, Session Facilitators, volunteers, trustees, service users, consultants & advisors
Relevant Legislation & Statutory Guidance	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Data (Use and Access) Act 2025 (DUAA 2025)

Brighter Together

Creating connections that light up lives

Definitions

Term	Definition
Charity	means Brighter Together, a registered charity (1190557).
Automated decision-making (ADM)	means decisions made solely by automated means, without human involvement, which have legal or similarly significant effects on individuals.
GDPR	means the UK General Data Protection Regulation as tailored by the Data Protection Act 2018 and the Data (Use and Access) Act 2025.
Responsible Person / Data Protection Lead	means the Chief Executive (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 any third party responsible for processing personal data on behalf of a controller.
Personal Data	Personal data means any information relating to a living person who can be identified, whether directly or indirectly. Information with identifiers removed but still linkable remains personal data; truly anonymous data is not.
Processing	Processing means anything done to or with personal data, including collecting, storing or deleting.
Special category data	The most sensitive types of personal data, e.g., health, race, religion.

1) Purpose

We protect people's personal data and comply with UK data protection law. This policy explains what that means in practice and sets out everyone's responsibilities.

2) Scope

This policy covers all personal data we handle in any format (paper or digital) about:

- Beneficiaries (including children and older adults)
- Staff, volunteers, session facilitators and trustees

- Donors, supporters and partners
- Any other individuals whose data we hold

It sits alongside our procedures: Privacy Notices, Register of Systems (data map), Retention Schedule, Breach Response Procedure, DPIA Procedure, IT Security Standard, and Complaints Policy.

3) Roles and responsibilities

- Trustees: Accountable for compliance; approve this policy and receive annual assurance.
- Data Protection Lead (DPL): The Chief Executive (or delegate). Maintains the Register of Systems; advises on lawful bases, DPIAs, contracts with processors, international transfers and breaches.
- Managers: Ensure team compliance, complete data mapping, and keep records up to date.
- Everyone (staff, volunteers, contractors): Follow this policy and our procedures, complete training, report incidents immediately.

Contact for data protection matters: dataprotection@brightertogether.org.uk

4) Our data protection principles

We follow the UK GDPR principles. Personal data must be:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

5) Lawful bases we rely on (overview)

We only process personal data where a lawful basis applies. The most common in our work are:

- Legitimate interests (e.g., running our programmes; stewardship of supporters where privacy impact is low and people would reasonably expect it)
- Consent (e.g., certain types of marketing; using photos or stories in publicity)
- Contract (e.g., paying a facilitator; volunteer agreements where applicable)
- Legal obligation (e.g., employment, tax, safeguarding)
- Vital interests (e.g., emergencies affecting health or safety)

The Register of Systems records the purpose and lawful basis for each processing activity and is reviewed at least annually. For electronic marketing we also follow PECR; people can opt out at any time.

6) Special category and criminal offence data

Where we handle special category data (e.g., health, ethnicity, religion, sexual orientation) we ensure we have both a lawful basis and a valid special condition (e.g., explicit consent, vital interests, employment law, substantial public interest, not-for-profit membership). We only handle criminal offence data where strictly necessary and with appropriate safeguards.

7) Children and safeguarding

We work with children and young people. We use extra care to ensure:

Deleted: sometimes

- Clear, child-friendly privacy information
- Consent from the child where appropriate (recognising that under 13s cannot give their own consent for information society services)
- Safeguarding first: if we must share data to protect a child or adult at risk, we do so lawfully and proportionately

8) Being open and fair (transparency)

We provide privacy information at the point of collection that explains: who we are, what we collect, why, our lawful basis, who we share data with, how long we keep it, people's rights and how to contact us. We keep our privacy notices short, plain-English, and easy to find.

9) Individual rights

People can exercise their UK GDPR rights:

- Access (a copy of their data)
- Rectification
- Erasure
- Restriction
- Objection (including to direct marketing)
- Data portability (where applicable)
- Rights relating to automated decision-making (we do not use ADM—see §13)

Requests should be sent to the DPL. We respond within one month (extendable by two months for complex requests). We verify identity where needed and keep a record of requests and outcomes.

10) Retention

We do not keep data longer than necessary. The Retention Schedule sets periods for each record type (e.g., beneficiary records, HR files, finance, safeguarding). When a period ends, we securely delete or anonymise the data. We keep a log of routine disposals.

11) Security

We use appropriate technical and organisational measures to keep data secure, including (as proportionate to risk):

- Access control and least-privilege permissions
- Strong authentication and device encryption
- Secure configuration, patching and malware protection
- Approved systems for storage and messaging; no unapproved personal accounts
- Regular backups and tested recovery
- Training, confidentiality undertakings and clear-desk/clear-screen practice
- Secure destruction of paper and media

Details live in our IT Security Standard.

12) Sharing data and using suppliers

We only share personal data when necessary and lawful, with proportionate safeguards. We use written contracts with all processors (suppliers who process data for us) that meet UK GDPR requirements.

International transfers outside the UK/EEA use approved safeguards (e.g., the UK IDTA or the UK addendum to the EU SCCs), plus transfer risk assessments where needed.

A current list of key processors and sharing partners is maintained in the Register of Systems and referenced in our privacy notices.

13) Automated decision-making (ADM)

We do not make decisions with legal or similarly significant effects solely by automated means. If this changes, we will update this policy, carry out a DPIA, and inform affected individuals with information about their rights.

14) Data Protection Impact Assessments (DPIAs)

We conduct a DPIA before starting any high-risk processing (for example: new technology, large-scale use of sensitive data, monitoring, children's data at scale, or non-routine data sharing). The DPL advises and records outcomes and mitigations.

15) Data breaches

A personal data breach is any security incident that affects confidentiality, integrity, or availability (e.g., loss, unauthorised access, ransomware, sending to the wrong person).

- Report immediately to the DPL (no blame culture).
- We assess risk and, if required, notify the ICO within 72 hours and affected individuals without undue delay.
- We record all breaches and near-misses and implement lessons learned.

Operational steps are set out in our Breach Response Procedure.

16) Training and assurance

- Mandatory induction and refresher training at least every 2 years (more often for higher-risk roles).
- Annual review of the Register of Systems, retention schedule and key supplier contracts.
- Periodic spot checks and audits proportionate to our size and risk.
- Trustees receive an annual compliance report from the DPL.

17) Complaints and contact

Questions, concerns or complaints about our data use can be sent to the DPL at dataprotection@brightertogether.org.uk. If we can't resolve a concern, individuals can contact the Information Commissioner's Office (ICO).

18) Document control

First adopted: 01 September 2020

Latest approval: 09 March 2026

Next scheduled review: 0 March 2028

Signed (for the Trustees): _____ (Chair)

Name: Andrew Melia, Chair of Trustees

Date: _____

Brighter Together

Creating connections that light up lives

Appendix A — Retention Schedule

These are default retention periods. Where law or guidance requires longer retention (e.g., safeguarding, litigation), we keep records for as long as necessary. Disposal means secure deletion or shredding/anonymisation as appropriate.

Record category	Examples	Typical lawful basis	Retention period	Notes
Board & Governance	Trustee board minutes, resolutions, registers	Legitimate interests / Legal obligation	Permanent	Historical record and governance evidence
Policies & Procedures	Approved policies, key procedures	Legitimate interests / Legal obligation	Current + 6 years	Audit trail and accountability
Beneficiary records	Contact details, support notes, attendance	Legitimate interests / Vital interests	6 years from last contact	Limitation period for claims
Safeguarding (beneficiaries)	Concerns, referrals, case files	Legal obligation / Vital interests / Substantial public interest	Minimum 6 years after case closure; longer if required (e.g., until age 25 for child records)	Follow safeguarding guidance; extend if investigation/litigation ongoing
Donors & supporters	Contact details, donation history, preferences	Legitimate interests / Consent (marketing)	Up to 6 years after last donation or interaction (longer for Gift Aid)	HMRC/audit and stewardship
Gift Aid records	Declarations and transaction data	Legal obligation	6 years after end of financial year	HMRC requirement
Finance (general)	Invoices, bank records, ledgers	Legal obligation	6 years after financial year end	Companies Act/HMRC

Employees	HR file, contracts, reviews	Contract / Legal obligation	6 years after employment ends	Limitation period; defend legal claims
Recruitment (unsuccessful)	Applications, interview notes	Legitimate interests	6 months (up to 12 months for safeguarding roles)	Fair recruitment; defend claims
Volunteers & facilitators	Application, references, agreements	Legitimate interests / Contract	3 years after role ends (longer if safeguarding issues)	Operational need; defend claims
Training records	Mandatory training completion	Legitimate interests / Legal obligation	6 years	Audit and compliance evidence
Health & Safety	Incident/accident reports, RIDDOR	Legal obligation	At least 3 years (longer for serious incidents; for children, until 21)	H&S regulations and claims
Images & stories (consented)	Photos, videos, case studies	Consent / Legitimate interests	Until consent withdrawn or 5 years (review before reuse)	Renew consent for new campaigns
IT & security logs	Access, audit, system logs	Legitimate interests / Legal obligation	12 months (longer if under investigation)	Security monitoring and incident response
Supplier/processor contracts	MSAs, DPAs, due diligence	Legal obligation / Contract	Contract term + 6 years	Audit and claims

Appendix B — Data Breach Response Procedure

Purpose: Provide a clear, rapid process for handling personal data breaches, meeting the 72-hour ICO reporting window where required.

1. Recognise & report (Immediate)

- Anyone who suspects a breach (loss, unauthorised access, mis-send, ransomware, etc.) must report it immediately to their manager and the DPL at dataprotection@brightertogether.org.uk.
- Do not attempt to fix or delete evidence before reporting. Take a screenshot or note what happened.

2. Contain & secure (Within hours)

- IT to isolate affected devices/accounts, reset credentials, revoke access, and block malicious activity.
- Retrieve/recall mis-sent emails where possible; ask unintended recipients to delete and confirm deletion.
- Preserve logs and relevant evidence.

3. Assess risk (Same day)

- DPL logs the incident and assesses the likelihood and severity of risk to individuals' rights and freedoms (consider sensitivity, volume, identifiability, vulnerability).
- Decide if the breach is notifiable to the ICO (likely risk) and/or requires communication to affected individuals (high risk).

4. Notify if required (Within 72 hours)

- If notifiable, DPL submits an ICO report within 72 hours of awareness, including: what happened, categories/approximate numbers of individuals and records, likely consequences, contact point, and measures taken/plan to mitigate.
- Where high risk to individuals, notify them without undue delay in clear language, including steps they should take.

5. Remediate & learn (Asap, then post-incident)

- Remedial actions (patches, process changes, training, contract updates) are assigned and tracked to completion.
- DPL records full details, decisions and rationales in the breach log. Trustees receive a summary of significant incidents.

Severity guide (examples)

- Low: limited internal exposure; promptly contained; minimal personal data; unlikely risk.
- Medium: personal data sent to unintended party or exposed briefly; potential inconvenience to individuals.
- High: sensitive/special category data, identity data, children's data, or large volumes; risk of harm — consider ICO notification and contact individuals.

Records kept

- Incident description, timeline and containment steps

- Risk assessment and decision on notification
- Notifications sent (ICO/individuals) with timestamps
- Actions taken and lessons learned

Brighter Together

Creating connections that light up lives

Appendix C — DPIA Template

Use this form before starting any high-risk processing or when introducing new technology or data sharing.

Project/Activity

- Name and brief description
- Owner and team
- Start date / planned go-live

Purpose and necessity

- What is the purpose and expected benefit?
- Why is personal data needed? (Consider data minimisation)

Data details

- Categories of data subjects (e.g., beneficiaries, staff, children)
- Categories of personal data (incl. special category/criminal offence)
- Sources of data and collection methods
- Estimated volumes and retention period

Lawful basis & special condition

- Lawful basis under UK GDPR
- Special condition for special category/criminal offence data (if any)

Data flows & sharing

- Diagram or description of data flows
- Processors/third parties and contracts in place
- International transfers and safeguards (IDTA/SCCs)

Risk assessment

- Identify risks to individuals (confidentiality, integrity, availability)
- Likelihood and impact (low/medium/high)
- Mitigations and residual risk

Consultation

- Views of stakeholders (e.g., beneficiaries, staff)
- Consultation with DPL and (if relevant) ICO

Outcomes & actions

- Go/no-go decision and rationale
- Actions, owners and deadlines

Approvals

- Project owner signature/date
- DPL review signature/date
- Trustee or senior approval (if required)