Data Protection Policy

1. Purpose of this Policy

The Brotherhood Charity ("the charity") collects, stores, and processes personal data about beneficiaries, trustees, volunteers, and partners.

This policy ensures that we handle personal data lawfully, fairly, and transparently, in compliance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations (PECR)

2. Scope

This policy applies to:

- All trustees, staff, and volunteers who handle personal data on behalf of the charity.
- All personal data collected via *The Brotherhood Charity*, events, forms, or communications.

3. Key Principles

We will follow the six UK GDPR principles, ensuring personal data is:

1. **Processed lawfully, fairly, and transparently**
2. **Collected for specified, explicit, and legitimate purposes**
3. **Adequate, relevant, and limited** to what is necessary
4. **Accurate and kept up to date**
5. **Stored only as long as necessary**
6. **Kept secure**

4. What Data We Collect

We may collect:

- Contact details (name, email, phone, postal address)
- Demographic information (age, service branch, veteran/serving status)
- Mental health and wellbeing information (only with explicit consent)
- Communication preferences
- Records of interactions with the charity

5. Lawful Basis for Processing

We will only process personal data when one of the following applies:

- **Consent** – the individual has given clear permission.
- **Contract** – processing is necessary for a service the individual has requested.
- **Legal obligation** – compliance with the law.
- **Vital interests** – to protect someone's life (e.g., suicide risk intervention).
- **Legitimate interests** – for purposes that are fair, balanced, and do not unduly impact the individual's rights.

6. Special Category Data

We may process sensitive information (e.g., mental health data) only where:

- The individual has given explicit consent, or
- Processing is necessary for safeguarding or protecting vital interests, or
- It is required by law.

Such data will be stored securely and accessed only by authorised personnel.

7. Data Security

We will:

- Store paper records in locked cabinets.
- Use password-protected systems for electronic data.
- Limit access to authorised trustees, staff, or volunteers.
- Encrypt sensitive digital files where possible.
- Train all personnel in data protection responsibilities.

8. Data Retention

- Personal data will only be kept for as long as necessary for its purpose.
- Safeguarding and case records will normally be kept for 6 years after closure.
- Basic contact information may be retained for ongoing communications unless consent is withdrawn.

9. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion of data (where lawful)
- Restrict or object to processing
- Request data portability
- Withdraw consent at any time

Requests should be made in writing to the charity's Data Protection Officer (DPO).

10. Data Breaches

Any data breach must be reported immediately to the DPO.
The DPO will assess the risk, take remedial action, and, where required, notify the Information Commissioner's Office (ICO) within 72 hours.

11. Data Protection Officer (DPO)

The DPO is responsible for:

- Ensuring compliance with this policy
- Acting as the contact point for data protection queries
- Maintaining the Data Protection Register

12. Review

This policy will be reviewed annually or when relevant legislation changes.

Policy last reviewed: Jan 2026