

4.3 Data Protection Policy (UK GDPR)

Charity Name: FOUNTAIN COMMUNITY PROJECT (FCP)

Charity Number: 1206682

Legal Structure: Charitable Incorporated Organisation (CIO)

Registered Address: Clody House, 1st Floor, Suite A, 90–100 Collingdon Street, Luton, LU1 1RX

Date Created: 23 January 2023

Last Updated: 01 May 2026

1. POLICY STATEMENT

Fountain Community Project is committed to protecting the personal data of all individuals who engage with our services.

We process personal data in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Best practice guidance for charities

We ensure that personal information is:

- Used fairly and lawfully
 - Kept secure and confidential
 - Only collected for specified and legitimate purposes
 - Retained only for as long as necessary
-

2. SCOPE

This policy applies to:

- Trustees
- Staff (paid and unpaid)
- Volunteers
- Contractors
- Service users (children, young people, families, vulnerable adults)

It covers all data collected through:

- Education programmes
 - Food distribution services
 - Community cohesion activities
 - Online systems and communications
 - Paper records and digital systems
-

3. TYPES OF DATA WE COLLECT

We may collect and process:

Personal Data:

- Names
- Addresses
- Contact details (phone, email)
- Date of birth

Sensitive (Special Category) Data:

- Health information (where relevant for safeguarding or education access)
- Safeguarding records
- Vulnerability status
- Free school meal / benefits eligibility (e.g. Universal Credit)

4. LEGAL BASIS FOR PROCESSING DATA

We only process data where there is a lawful basis:

- Consent (where applicable)
- Contract (service delivery agreements)
- Legal obligation (safeguarding and compliance)
- Legitimate interest (charitable service delivery)
- Vital interests (emergency safeguarding situations)

5. DATA USE

We use personal data to:

- Deliver education programmes
- Manage food distribution services
- Support youth mentoring and community programmes
- Safeguard children and vulnerable individuals
- Communicate with service users and partners
- Manage volunteers and trustees

6. DATA SECURITY

We ensure data is protected through:

- Password-protected systems
- Restricted access to sensitive files
- Secure storage of paper records
- Encryption where possible
- Staff and volunteer training on confidentiality

Access is limited to those who need it for their role.

7. DATA SHARING

We may share data only when necessary with:

- Safeguarding authorities
- Schools and education providers
- Local authorities (e.g. Luton Borough Council)
- Police (e.g. Bedfordshire Police where safeguarding requires)
- Partner charities (e.g. foodbanks and shelters)

We will never sell personal data.

8. DATA RETENTION

We retain data only as long as necessary:

- Safeguarding records: retained securely in line with legal requirements
- Service user records: retained for service delivery duration + review period
- Volunteer and trustee records: retained during role + limited period after

After retention periods, data is securely deleted or destroyed.

9. INDIVIDUAL RIGHTS

Under UK GDPR, individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion (where applicable)
- Restrict or object to processing
- Data portability (where relevant)

Requests should be made to the Data Protection Lead.

10. DATA BREACHES

In the event of a data breach:

- It will be reported immediately to the Data Protection Lead
 - Risk will be assessed
 - If necessary, the Information Commissioner's Office (ICO) will be notified within 72 hours
 - Affected individuals will be informed if required
-

11. ROLES AND RESPONSIBILITIES

Trustees:

- Ensure compliance with data protection law
- Oversee governance and risk

Data Protection Lead:

- Manage day-to-day compliance
- Handle data requests and breaches
- Maintain records of processing activities

Staff and Volunteers:

- Follow data handling procedures
 - Report any suspected breaches immediately
 - Maintain confidentiality at all times
-

12. TRAINING

All trustees, staff, and volunteers must:

- Receive data protection awareness training
 - Understand GDPR principles relevant to their role
 - Follow secure handling procedures
-

13. DOCUMENT CONTROL

- **Document Owner:** Data Protection Lead
- **Approved By:** Board of Trustees

- Review Frequency: Annual
 - Next Review Date: 01 May 2027
-