StrongRootzProject Data Protection Policy

Policy Date: September 2025
Next Review Date: September 2026

1. Introduction

StrongRootzProject is committed to protecting the personal data of all children, parents/carers, staff, volunteers, and other stakeholders. This policy outlines how we collect, store, process, and share data in compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

This policy applies to all staff, mentors, volunteers, and contractors handling personal data.

2. Policy Objectives

- Ensure compliance with data protection legislation.
- Protect the privacy and rights of children and stakeholders.
- Ensure personal data is processed lawfully, fairly, and transparently.
- Minimise the risk of data breaches.
- Provide guidance on handling, storage, and sharing of data.

3. Data Protection Principles

StrongRootzProject will adhere to the following principles:

1. **Lawfulness, Fairness, and Transparency:** Personal data is processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation:** Data is collected for specified, explicit, and legitimate purposes.
3. **Data Minimisation:** Only necessary data is collected and processed.
4. **Accuracy:** Personal data is accurate and kept up to date.
5. **Storage Limitation:** Data is kept only as long as necessary for its purpose.
6. **Integrity and Confidentiality:** Data is processed securely to protect against unauthorised access, loss, or damage.
7. **Accountability:** StrongRootzProject can demonstrate compliance with all data protection principles.

4. Types of Data Collected

We may collect and process:

- Personal details (name, date of birth, address, contact details).

- Educational information (school, year group, learning needs).
- Safeguarding records (concerns, incidents, referrals).
- Attendance records.
- Staff, volunteer, and mentor records (contracts, references, DBS checks).
- Communications (emails, phone calls, messages) relevant to mentoring activities.

5. Lawful Basis for Processing

We process personal data under one or more lawful bases:

- **Consent:** Explicit consent from parents/carers or participants where appropriate.
- **Legal Obligation:** To comply with safeguarding, employment, or statutory requirements.
- **Legitimate Interests:** To deliver mentoring services effectively.
- **Vital Interests:** To protect a child's safety or welfare in emergencies.

6. Data Storage and Security

- All data is stored securely in password-protected digital systems or locked physical storage.
- Access is restricted to staff and mentors who require it for their role.

- Regular backups are maintained, and sensitive data is encrypted where possible.
- Devices used to access data (computers, tablets, phones) must be password-protected and updated with security software.

7. Data Sharing

- Personal data is only shared with consent or where legally required (e.g., Children's Social Care, Police, Ofsted).
- Information sharing follows the **"Seven Golden Rules" of information sharing** as outlined in **Working Together to Safeguard Children (2018)**.
- Any data shared outside the service must be done securely (encrypted email, secure portals).

8. Data Retention

- Personal data is retained only as long as necessary for its purpose, including statutory obligations.
- Safeguarding records are retained in line with legal and best-practice requirements.
- Once retention periods expire, data is securely deleted or destroyed.

9. Individual Rights

Individuals have the right to:

- Access their personal data (Subject Access Request).
- Request correction of inaccurate data.
- Request erasure of personal data ("right to be forgotten") where appropriate.
- Restrict or object to processing.
- Request data portability.

Requests should be made to the **Data Protection Lead/ Safeguarding Lead**.

10. Data Breaches

- Any data breach must be reported immediately to the **Data Protection Lead**.
- The lead will assess the risk to individuals and notify the **Information Commissioner's Office (ICO)** within 72 hours if required.
- Breaches are recorded and reviewed to prevent recurrence.

11. Staff and Mentor Responsibilities

All staff and mentors must:

- Handle data responsibly and only for legitimate purposes.
- Maintain confidentiality at all times.

- Complete mandatory data protection and GDPR awareness training.
- Report any data breaches or potential issues immediately.

12. Monitoring and Review

- This policy is reviewed annually or sooner if legislation changes.
- **Next review date: September 2026**
- The Safeguarding Lead / Data Protection Lead ensures staff are informed of updates.

Policy Approved By: J Johnston, Founder & Director.
Date: September 2025