Data Protection Policy

1. Purpose

Engage Community collects, stores, and processes personal information about children, families, staff, volunteers, and partners. This policy sets out how we protect personal data in compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and other relevant legislation.

Our commitment is to ensure that all personal data is handled securely, lawfully, and transparently to protect the rights and privacy of individuals.

---

2. Scope

This policy applies to:

- All staff, coaches, and volunteers.
- Trustees, contractors, and anyone handling data on behalf of Engage Community.
- All personal data, whether stored digitally, on paper, or shared verbally.

---

3. Data Protection Principles

In line with UK GDPR, Engage Community commits to processing personal data according to the following principles:

1. **Lawfulness, fairness, and transparency** – Data will be processed fairly and individuals will be informed of how their data is used.
2. **Purpose limitation** – Data will only be collected for specified, explicit, and legitimate purposes.
3. **Data minimisation** – Only the data necessary for the intended purpose will be collected.
4. **Accuracy** – Data will be accurate and kept up to date.
5. **Storage limitation** – Data will be kept only as long as necessary.
6. **Integrity and confidentiality** – Data will be kept secure and protected from unauthorised access or loss.
7. **Accountability** – Engage Community will take responsibility for how data is managed and demonstrate compliance with data protection laws.

---

4. Types of Data We Collect

- **Children and families:** contact details, emergency contacts, medical information, safeguarding records, attendance registers, consent forms.

- **Staff and volunteers:** contact details, employment records, references, DBS checks, training records.
- **Partners and stakeholders:** contact details, contracts, agreements.

---

5. Lawful Basis for Processing

Engage Community will only process personal data where a lawful basis exists, including:

- **Consent** (e.g., parental consent for photography).
- **Contract** (e.g., employment contracts).
- **Legal obligation** (e.g., safeguarding requirements, HMRC reporting).
- **Vital interests** (e.g., medical emergencies).
- **Legitimate interests** (e.g., organisational administration).

---

6. Data Storage and Security

- Digital data is stored securely with password protection and restricted access.
- Paper records are kept in locked cabinets in secure offices.
- Data is only accessible to those who need it for their role.
- Staff and volunteers must not store personal data on personal devices unless authorised and protected.
- Any data breaches will be reported in line with the ICO's breach reporting requirements.

---

7. Data Sharing

We will only share personal data where necessary and lawful, for example:

- With emergency services in a safeguarding or medical emergency.
- With statutory bodies (e.g., Ofsted, Social Care, DBS).
- With trusted third-party service providers who comply with data protection law.
  We will never sell personal data to third parties.

---

8. Data Retention

Personal data will not be kept longer than necessary. Engage Community follows sector-specific guidance on retention periods (e.g., safeguarding records are kept until the child reaches the age of 25). A **Data Retention Schedule** is maintained and reviewed annually.

---

9. Individual Rights

All individuals have the following rights under UK GDPR:

- The right to be informed about how their data is used.
- The right of access to their personal data.
- The right to rectification of inaccurate or incomplete data.
- The right to erasure (where applicable).
- The right to restrict processing.
- The right to data portability.
- The right to object to processing.
- Rights relating to automated decision making and profiling (not applicable to Engage Community).

Requests to exercise these rights should be submitted in writing to the **Data Protection Lead**. Engage Community will respond within **one month**.

---

10. Roles and Responsibilities

- **Data Protection Lead (DPL):** [Insert Name/Role] – responsible for overseeing compliance and handling subject access requests.
- **Staff and volunteers:** must follow this policy, only use data for legitimate purposes, and report breaches immediately.
- **Trustees:** ensure oversight and compliance with data protection legislation.

---

11. Breach Management

- Any suspected data breach must be reported immediately to the DPL.
- Serious breaches will be reported to the **Information Commissioner's Office (ICO)** within 72 hours, as required by law.
- Affected individuals will be informed where there is a high risk to their rights and freedoms.

---

12. Policy Review

This policy will be reviewed annually or sooner if legislation or organisational practice changes.

Adopted by Engage Community
Date: 01.09.2025
Signed: M Price