Brenda Keirnan 29/09/2025

Forming Connections

Data Protection Policy

Last reviewed: 25/09/2025
Next review due: 25/09/2026
Policy owner: Education Director
Applies to: All staff, contractors, volunteers, associates, and trustees

---

1. Policy Statement

Forming Connections is committed to protecting the personal data of everyone we work with including children, young people, vulnerable adults, parents, staff, and partners.

We recognise that people trust us with their information, and we take this responsibility seriously. We comply with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, ensuring that personal data is collected, stored, processed, and shared safely, lawfully, and transparently.

This policy sets out how we manage personal data in line with our values of **safety, relational integrity, and inclusion**.

---

2. Purpose

The purpose of this policy is to:

- Ensure compliance with UK data protection laws
- Protect the rights and privacy of individuals whose data we process
- Establish clear standards for staff, volunteers, and contractors handling personal data
- Support safe and secure working practices in education and safeguarding contexts

---

3. Scope

This policy applies to all personal data processed by Forming Connections in any format, including:

- Digital files, emails, and online forms
- Paper records, notes, and sign-in sheets
- Images, videos, and recordings
- Data collected in person, by phone, or online

It applies to all employees, contractors, volunteers, associates, and trustees.

4. Legal Framework

This policy is based on the following legislation and guidance:

- **UK GDPR (2018)**
- **Data Protection Act 2018**
- **Human Rights Act 1998**
- **Freedom of Information Act 2000** (where applicable)
- **Children Act 1989 & 2004** (information sharing for safeguarding)
- Statutory safeguarding guidance (*Working Together to Safeguard Children 2018*)

---

5. Key Data Protection Principles

Forming Connections adheres to the **7 key principles of data protection** under UK GDPR:

1. **Lawfulness, fairness & transparency**: We process data lawfully and explain clearly why and how we use it.
2. **Purpose limitation**: Data is collected for specific, legitimate purposes only.
3. **Data minimisation**: We collect only the data we genuinely need.
4. **Accuracy**: We keep personal data accurate and up to date.
5. **Storage limitation**: We don't keep personal data longer than necessary.
6. **Integrity and confidentiality**: We keep personal data secure.
7. **Accountability**: We take responsibility for how we handle data and can demonstrate compliance.

---

6. Types of Personal Data We Collect

Depending on our activities, we may collect:

- **Basic contact details**: names, addresses, emails, phone numbers
- **Professional information**: job titles, employer details, training records
- **Participant information**: age, learning needs, support requirements
- **Safeguarding information**: where there are concerns or incidents
- **Staff & contractor data**: for recruitment, DBS, payroll, and compliance
- **Photographs or recordings**: used only with consent

We collect **special category data** (e.g. health, safeguarding information) only where necessary and with appropriate safeguards.

---

7. Lawful Bases for Processing

We process personal data under one or more of the following lawful bases:

- **Consent**: when individuals give clear permission (e.g. email lists, photos)
- **Contract**: when processing is necessary to deliver our services
- **Legal obligation**: e.g. safeguarding records, employment law, HMRC
- **Vital interests**: to protect someone's life in an emergency
- **Public task**: when carrying out functions in the public interest (e.g. safeguarding referrals)
- **Legitimate interests**: where processing is necessary for our legitimate business purposes, balanced against individuals' rights

For special category data, we rely on additional conditions, such as safeguarding or explicit consent.

---

8. Information Sharing

We only share personal information when it is:

- Necessary for safeguarding or legal reasons
- Required by law (e.g. police, local authority)
- With explicit consent
- With trusted third-party processors under strict data processing agreements

We never sell personal data to third parties.

---

9. Data Storage and Security

We take appropriate measures to keep personal data secure, including:

- **Password-protected and encrypted systems**
- **Secure cloud storage** with UK GDPR-compliant providers
- **Limited access** to data based on role
- **Locked filing cabinets** for paper records
- **Data retention schedules** and regular reviews

All staff are required to follow security procedures and report any breaches immediately.

---

10. Retention and Deletion

We keep personal data only for as long as necessary to fulfil the purposes for which it was collected and to comply with legal obligations.

Typical retention periods include:

- Safeguarding records: **up to 25 years** (depending on case)
- Staff and contractor records: **6 years** after employment ends
- Participant records: **3–7 years** depending on programme
- Financial records: **6 years** (HMRC requirement)

At the end of the retention period, data is securely deleted or destroyed.

---

11. Data Subject Rights

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access (Subject Access Request)
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making (not currently used by Forming Connections)

Requests should be made in writing to the **Data Protection Lead**. We will respond within **one month**.

---

12. Data Breaches

A data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

- All breaches must be reported immediately to the Data Protection Lead.
- Serious breaches will be reported to the **Information Commissioner's Office (ICO)** within **72 hours**, where legally required.
- We will notify affected individuals if the breach poses a high risk to their rights and freedoms.

---

13. Roles and Responsibilities

- **Education Director / Data Protection Lead**
  - Overall responsibility for data protection compliance
  - Maintains records of processing activities
  - Acts as contact point with the ICO
- **All staff, volunteers, and contractors**
  - Must follow this policy and data protection training
  - Report breaches or concerns immediately

---

14. Policy Review

This policy is reviewed annually, or sooner if required by changes in legislation, guidance, or organisational practice.

All staff must read, understand, and comply with this policy as part of their induction and ongoing responsibilities.

Approved by:

Name: Brenda Keirnan
Role: Education Director
Date: 29/09/2025