



The Seeds of Change KMD Ltd

Data Protection Policy

Policy Version: 2025–2026

© The Seeds of Change KMD Ltd | Page 1 of 6

1. Policy Statement

The Seeds of Change (TSOC) is committed to protecting the privacy and security of all personal data we process.

We recognise our responsibility under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018** to ensure that any personal data relating to children, parents, carers, staff, and referring organisations is handled lawfully, fairly, and transparently.

This policy sets out how we collect, use, store, and share personal data in compliance with current UK data protection law.

We are registered with the **Information Commissioner's Office (ICO)** as a data controller.

2. Scope

This policy applies to:

- All employees, volunteers, and contractors of The Seeds of Change
- All personal data processed by or on behalf of TSOC, including digital and paper records
- All data relating to children, young people, parents, carers, referring organisations, staff, and suppliers

It covers all forms of data handling within our provision, including:

- Referrals and enrolment
- Safeguarding and welfare records
- Attendance and progress tracking
- Equine-assisted learning outcomes
- Personnel and HR data
- CCTV (if used) and photography

3. Legal Framework

This policy complies with the following legislation and statutory guidance:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Education Act 1996 & 2002**
- **Children Act 1989 & 2004**
- **Keeping Children Safe in Education (2025)**
- **Human Rights Act 1998 (Article 8 – Right to Privacy)**
- **Freedom of Information Act 2000**

4. Data Protection Principles

In accordance with Article 5 of the UK GDPR, TSoC ensures that all personal data is:

1. **Processed lawfully, fairly and transparently** – we explain what we do with personal data and why.
2. **Collected for specified, explicit and legitimate purposes** – data is only used for educational, therapeutic, or safeguarding purposes.
3. **Adequate, relevant and limited** – only the data necessary to fulfil our duties is collected.
4. **Accurate and kept up to date** – we ensure data accuracy and correct errors promptly.
5. **Stored for no longer than necessary** – we follow defined retention schedules.
6. **Processed securely** – we use appropriate technical and organisational measures to protect data.

5. Lawful Bases for Processing

TSoC will only process personal data when there is a lawful basis under Article 6 of the UK GDPR, including:

- **Consent:** e.g. for using photographs or testimonials.
- **Contract:** processing necessary for an employment or service contract.
- **Legal obligation:** e.g. safeguarding and attendance reporting.
- **Vital interests:** e.g. in a medical emergency.
- **Public task:** for the delivery of education or training in the public interest.
- **Legitimate interests:** e.g. internal record-keeping and quality monitoring.

For **special category data** (e.g. health, ethnicity, or SEN data), additional conditions under Article 9 apply — such as the substantial public interest for safeguarding and equal opportunity monitoring.

6. Types of Personal Data We Collect

We collect and process data including, but not limited to:

For learners:

- Name, date of birth, address, contact details
- Education history, referring body, attendance records
- Medical information and emergency contacts
- SEND or EHCP information
- Photographs (for identification or progress purposes)
- Safeguarding and behavioural information

For parents/carers/referring bodies:

- Contact details
- Relationship to the learner
- Relevant safeguarding or pastoral information

For staff and volunteers:

- Recruitment and employment details
 - DBS and safeguarding records
 - Training and performance data
 - Payroll and emergency contact information
-

7. Data Sharing

TSoC shares data only when necessary and lawful, and always in line with the **‘need to know’** principle.

We may share data with:

- Referring schools, local authorities, and Virtual School Heads
- Safeguarding partners and Children’s Social Care
- The police or other statutory agencies (when required by law)
- Medical professionals in emergencies

- External trainers, therapists, or service providers under contract (with data protection agreements in place)

We **do not** share or sell personal data to third parties for marketing purposes.

Where we share data with external processors, **Data Processing Agreements** are in place to ensure compliance with the UK GDPR.

8. Data Storage and Security

We take robust technical and organisational measures to protect data, including:

- Secure password-protected electronic systems (Google Workspace for Education or equivalent)
- Encryption of devices containing personal data
- Locked filing cabinets for paper records
- Restricted access to confidential information (DSLs, Head of Centre, relevant staff only)
- Use of secure email or encrypted transfer for sensitive information
- Staff training on information security and data handling

In the event of a **data breach**, the DSL or Data Protection Lead will follow TSoC's **Data Breach Procedure**, notifying the ICO within 72 hours if required.

9. Retention and Disposal

Data will not be retained for longer than necessary.

Retention follows guidance from:

- The **Information and Records Management Society (IRMS) Education Retention Schedule (2024)**
- Statutory safeguarding and education requirements

Examples:

- **Safeguarding records:** retained until the child's 25th birthday
- **Personnel files:** retained for 6 years after employment ends
- **Financial records:** retained for 7 years

When data is no longer needed, it is securely destroyed or permanently deleted.


10. Data Subject Rights

Under the UK GDPR, individuals have the following rights:

- **To be informed** about how their data is used

- **To access** a copy of their personal data
- **To rectification** of inaccurate or incomplete data
- **To erasure ('right to be forgotten')** where applicable
- **To restrict processing** in certain circumstances
- **To data portability**
- **To object** to processing on specific grounds
- **Rights in relation to automated decision making and profiling**

Requests to exercise these rights should be made in writing to:

 info@theseedsofchange.co.uk (or the Data Protection Lead's direct address)

We will respond within **one calendar month**, unless the request is complex or excessive.

11. Photography, Video and Social Media

TSoC uses photography and video for educational, progress, and promotional purposes.

- Written consent is always obtained prior to use.
 - No images are published without appropriate permission.
 - Learners are never named in public posts or materials.
 - All media files are stored securely and deleted when no longer needed.
-

12. Data Breaches

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

In the event of a breach:

1. Staff must report it immediately to the **Data Protection Lead** or DSL.
 2. The incident will be investigated promptly.
 3. Where risk to individuals is likely, the ICO will be notified within 72 hours.
 4. Affected individuals will be informed without undue delay if there is a high risk to their rights or freedoms.
 5. Actions will be taken to prevent recurrence.
-

13. Roles and Responsibilities

- **Data Protection Lead (DPL):** Oversees data protection compliance, policy review, and breach management.

- **Designated Safeguarding Lead (DSL):** Ensures safeguarding data is stored and shared lawfully and securely.
- **All Staff and Volunteers:** Must follow this policy and attend annual data protection training.

Failure to follow this policy may result in disciplinary action.

14. Training and Awareness

All staff receive data protection and confidentiality training as part of induction and annual refreshers.

Specialist staff (DSLs, senior leaders, and admin staff) receive enhanced training relevant to their roles.

15. Monitoring and Review

This policy will be reviewed annually or sooner if legislation changes, under the supervision of the Data Protection Lead and the Senior Leadership Team.

Any significant data breaches, changes in law, or ICO recommendations will trigger an immediate review.

16. Related Policies

This policy links to:

- Safeguarding and Child Protection Policy
- Confidentiality Policy
- ICT and Online Safety Policy
- Safer Recruitment Policy
- Whistleblowing Policy
- Record Retention and Disposal Procedure

Document Owner: Head of Centre – Rebecca Perrin

Next Review Due: September 2026

Approved by: Senior Leadership Team