

Data Protection & GDPR Policy — Public Version

1. Purpose

Second Chances Intervention CIC (SCI) is committed to protecting the privacy and personal information of children, young people, families, staff and partners. This policy explains how SCI collects, uses, stores and shares personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Our Commitment

SCI ensures:

- Lawful, fair and transparent processing of personal data
- Secure storage and restricted access
- Clear information-sharing protocols
- Confidentiality across all practice
- Compliance with UK GDPR principles
- Respect for the rights of individuals

3. What Data We Collect

SCI may collect:

- Contact details (names, phone numbers, email addresses)
- Referral information from schools or local authorities
- Assessment information
- Intervention notes and progress reports
- Attendance records
- Safeguarding information
- Multi-agency meeting notes

- Staff training and supervision records

We only collect information necessary for delivering safe, effective intervention.

4. Lawful Basis for Processing

SCI processes data under the following lawful bases:

- **Public Task** — delivering services commissioned by schools or local authorities
- **Legitimate Interests** — providing SEMH intervention and safeguarding support
- **Legal Obligation** — safeguarding, reporting and statutory requirements
- **Consent** — where required for specific activities

5. How We Use Personal Data

SCI uses personal data to:

- Deliver SEMH intervention
- Monitor progress and outcomes
- Support safeguarding and risk management
- Communicate with schools, families and agencies
- Meet legal and statutory duties
- Improve service quality

6. Information Sharing

SCI shares information only when necessary and appropriate, including with:

- Schools, PRUs, APs and academy trusts
- Local authorities
- Social care

-
- Youth offending teams
 - Safeguarding partners
 - Emergency services (where required)

We never sell personal data or share it for marketing purposes.

7. Data Storage & Security

SCI stores data securely using:

- Encrypted digital systems
- Password-protected devices
- Restricted access for authorised staff only
- Secure record-keeping in line with safeguarding standards

Paper records (if used) are stored in locked cabinets within secure premises.

8. Data Retention

SCI retains data only for as long as necessary to fulfil its purpose and meet legal requirements. Retention periods vary depending on:

- Safeguarding relevance
- Commissioning requirements
- Statutory guidance

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

9. Your Rights

Under UK GDPR, individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion (where appropriate)

- Object to processing
- Request restriction of processing
- Request data portability

Requests can be made by contacting: allison@scintervention.co.uk

10. Data Breaches

SCI follows strict procedures for managing data breaches. If a breach poses a risk to individuals, SCI will notify the Information Commissioner's Office (ICO) and affected parties in line with legal requirements.

11. Review

This policy is reviewed annually or sooner if required by legislation or commissioning partners.