



Data Protection and Disposal Policy

1. Purpose

This policy sets out how Autism Mentors Ltd collects, processes, stores, and disposes of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Our aim is to ensure all data is handled lawfully, fairly, transparently, and securely to protect the privacy of clients, families, staff, and partners.

2. Scope

This policy applies to:

- All Autism Mentors staff, consultants, and contractors.
- All systems, devices, and records containing personal or sensitive information.
- All data relating to clients, families, employees, and third parties.

3. Legal and Regulatory Framework

This policy aligns with:

- UK GDPR
- Data Protection Act 2018
- Children Act 1989 & 2004
- Care Act 2014
- Keeping Children Safe in Education (KCSIE 2025)

- Working Together to Safeguard Children (2018)
- Oxfordshire County Council (OCC) Safeguarding and Data Sharing Guidelines

4. Data Protection Principles

Autism Mentors Ltd adheres to the seven principles of UK GDPR:

1. Lawfulness, fairness, and transparency – Data is processed lawfully and individuals are informed about its use.
2. Purpose limitation – Data is only used for legitimate purposes related to our services.
3. Data minimisation – Only the minimum necessary information is collected.
4. Accuracy – Data is kept accurate and up to date.
5. Storage limitation – Data is retained only as long as necessary.
6. Integrity and confidentiality – Data is stored securely and protected against loss or misuse.
7. Accountability – We take responsibility for demonstrating compliance with UK GDPR.

5. Data We Process

Autism Mentors Ltd processes the following categories of personal data:

Category	Examples	Lawful Basis
Client information	Names, DOB, contact details, education and care plans	Consent; Legitimate interest; Legal obligation
Sensitive data (Special category)	Medical, behavioural, and safeguarding information	Vital interests; Legal obligation; Substantial public interest

Employee data	Recruitment, DBS, payroll, training records	Contract; Legal obligation
Safeguarding records	Referrals, reports, outcomes	Legal obligation; Vital interests
Operational data	Schedules, correspondence, attendance logs	Legitimate interest

6. Data Collection and Processing

- Information is collected directly from clients, parents/carers, employees, and referring professionals.
- Consent is obtained where required and recorded in writing.
- Data sharing is limited to what is necessary for safeguarding, service delivery, and contractual compliance.

7. Data Storage and Security

- All electronic data is stored on encrypted, password-protected devices and secure cloud systems.
- Paper files are stored in locked cabinets with access limited to authorised staff.
- Emails containing personal data use secure professional accounts and encrypted attachments where necessary.
- Staff receive mandatory data protection and confidentiality training annually.

8. Data Retention

Type of Record	Retention Period	Rationale
Client records	2 year after end of service	Safeguarding and legal compliance
Safeguarding files	7 years minimum or until case closure plus review	Legal requirement
HR and recruitment data	6 years post-employment	Employment law
Financial records	7 years	HMRC compliance
Training and supervision logs	3 years	Best practice
Incident reports	7 years	Risk management

Retention is reviewed annually in line with OCC guidance and the company's Record of Processing Activities (ROPA).

9. Data Disposal and Destruction

When data is no longer required:

- Paper records are cross-shredded or securely disposed of by an approved contractor.
- Digital data is permanently deleted from systems and backups.
- Portable devices are securely wiped or destroyed before disposal or reissue.
- A Data Disposal Log is maintained for all destroyed records.

10. Data Breach Management

- Any data breach (loss, access, or misuse) must be reported immediately to the Designated Safeguarding Lead (DSL) / Data Protection Lead.
- Breaches are logged and investigated.
- Where a breach poses a risk to individuals, the ICO and affected parties will be notified within 72 hours, in line with GDPR Article 33.

Data Protection Lead:

Michelle Wray – Director, DSL & DPL

 dsl@autismmentors.co.uk |  07707 764876

11. Rights of Individuals

We uphold all data subject rights under UK GDPR:

- Right to be informed
- Right of access
- 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

Requests are acknowledged within 5 working days and responded to within one month.

12. Data Sharing

Data may be shared only when:

- There is a lawful basis (e.g. safeguarding, legal requirement, or consent).
- The recipient is verified (e.g. local authority, school, healthcare provider).
- A Data Sharing Agreement (DSA) or secure transfer method is used.

We do not share personal data for marketing or non-essential purposes.

13. Monitoring and Review

- This policy is reviewed annually by the Directors and Data Protection Lead.
- Training is updated to reflect any changes in legislation, OCC guidance, or ICO advice.
- Lessons learned from incidents or audits inform continuous improvement.

14. Approval and Sign-off

Approved by:

Michelle Wray – Director & DSL

Signature:



Date: 05/09/2025

Next Review: September 2026