



DATA PROTECTION POLICY 2025-2026

Reviewed: April 2025
Next Review due: April 2026
Approved by the Senior Leadership Team



Table of Contents

1. Introduction.....	2
2. Scope	2
3. Definitions.....	3
4. Data Protection Principles.....	3
5. Lawful Basis for Processing.....	3
6. Roles and Responsibilities	4
7. Data Collection and Use.....	4
8. Privacy Notices.....	5
9. Data Subject Rights.....	5
10. Data Sharing.....	5
11. Data Security	6
12. Data Retention	6
13. Data Breaches	6
14. Training	7
15. Third-Party Processors.....	7
16. Monitoring and Review	7
17. Consequences of Non-Compliance.....	7
18. Contact.....	7
19. Related Policies.....	8

1. Introduction

Bespoke Mentoring and Training Services Limited ("the Organisation") is an alternative provision delivering mentoring and training to learners aged 11-25 with special educational needs (SEN) and social, emotional, and mental health (SEMH) needs, and employing staff to support these services. We are committed to protecting the personal data of our learners and staff in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This policy outlines our procedures for collecting, processing, storing, and protecting personal data, with a focus on the sensitive nature of SEN and SEMH data, ensuring transparency, security, and respect for individual rights.

This policy applies to all employed staff, learners, and third parties processing personal data on behalf of the Organisation. It covers physical and digital data, ensuring safeguards for vulnerable learners and compliance with statutory obligations.

2. Scope

This policy covers:

- Personal data of learners aged 6-25, particularly special category data related to SEN (e.g., EHCPs, diagnoses) and SEMH (e.g., mental health records, behavioural plans).
- Personal data of employed staff, including employment records, contact details, and health data.
- Data processed by the Organisation as a data controller or via third-party data processors.
- All activities involving the collection, storage, use, sharing, and deletion of personal data.

3. Definitions

- **Personal Data:** Information relating to an identifiable individual (e.g., name, address, learner records).
- **Special Category Data:** Sensitive data, including health, ethnicity, SEN, SEMH, or biometric data, requiring enhanced protections.
- **Data Controller:** The Organisation, determining the purposes and means of processing personal data.
- **Data Processor:** Third parties processing data on our behalf (e.g., IT providers, assessment platforms).
- **Data Subject:** Individuals whose data is processed (e.g., learners, staff).

4. Data Protection Principles

The Organisation adheres to the six UK GDPR Privacy Principles:

1. **Lawfulness, Fairness, and Transparency:** Data is processed lawfully, fairly, and with clear communication to data subjects.
2. **Purpose Limitation:** Data is collected for specific, legitimate purposes (e.g., education, safeguarding) and not used incompatibly.
3. **Data Minimisation:** Only necessary data is collected, especially for sensitive SEN/SEMH records.
4. **Accuracy:** Data is kept accurate and updated, with mechanisms to correct inaccuracies promptly.
5. **Storage Limitation:** Data is retained only as long as required, per our retention policy.
6. **Integrity and Confidentiality:** Data is processed securely to prevent unauthorised access, loss, or damage.

5. Lawful Basis for Processing

We process personal data under the following lawful bases:

- **Public Task (Article 6(1)(e)):** Processing learner data to deliver education, SEN/SEMH support, and meet statutory duties (e.g., safeguarding, DfE reporting).
- **Contract (Article 6(1)(b)):** Processing staff data for employment purposes (e.g., payroll, HR records).

- **Legal Obligation (Article 6(1)(c)):** Sharing data with authorities (e.g., local safeguarding boards, DfE).
- **Consent (Article 6(1)(a)):** For non-essential uses (e.g., marketing, photos), with clear, informed consent, accessible to learners with SEN/SEMH.
- **Legitimate Interests (Article 6(1)(f)):** For limited purposes (e.g., internal reporting), ensuring no override of data subject rights.

For special category data (e.g., SEN, SEMH, health), we rely on:

- **Substantial Public Interest (Article 9(2)(g)):** For education, safeguarding, or equality monitoring, especially for SEN/SEMH support.
- **Employment Law (Article 9(2)(b)):** For staff health or welfare data.
- **Explicit Consent (Article 9(2)(a)):** Where required, with documented, accessible agreement (e.g., simplified formats for learners with SEN).

6. Roles and Responsibilities

- **Data Protection Officer (DPO):** Oversees compliance, advises on data protection, and serves as the contact for data subjects and the Information Commissioner's Office (ICO). Contact: laura.davis@bespokementoring.org
- **Senior Leadership Team:** Ensures policy implementation, staff training, and regular audits.
- **SENCO (Special Educational Needs Coordinator):** Ensures SEN/SEMH data is handled sensitively and aligned with EHCPs.
- **All Staff:** Comply with this policy, report breaches, and handle data securely. Staff handling SEN/SEMH data receive specialised training.
- **Learners and Parents/Carers:** Informed of their rights via accessible privacy notices and encouraged to raise concerns with the DPO.

7. Data Collection and Use

We collect data to:

- Deliver tailored education and mentoring for learners with SEN/SEMH (e.g., EHCPs, progress reports, behaviour plans).
- Support learner well-being (e.g., mental health records, safeguarding information).
- Manage staff employment (e.g., contracts, absence records, training logs).
- Meet statutory obligations (e.g., DfE census, local authority SEN reporting).

Data is collected via:

- Enrolment forms and EHCP documentation (learners).
- HR onboarding processes (staff).
- Referrals from local authorities or external agencies (e.g., CAMHS, social services).
- Direct input from data subjects (e.g., consent forms, health updates).

8. Privacy Notices

We provide accessible privacy notices tailored to:

- **Learners:** In age-appropriate, SEN-friendly formats (e.g., simplified language, visuals for ages 6-14, or audio for SEMH needs).
- **Parents/Carers:** For learners under 18 or those lacking capacity to understand.
- **Staff:** Provided during onboarding.

Notices detail:

- Types of data collected (e.g., SEN diagnoses, mental health records).
- Lawful basis and purposes of processing.
- Data sharing (e.g., with DfE, health services).
- Retention periods, rights, and complaint procedures.

Notices are available on our website, in accessible formats, and updated for significant changes.

9. Data Subject Rights

Data subjects (learners, staff, parents/carers) have the following UK GDPR rights:

- **Right to be Informed:** Via accessible privacy notices.
- **Right of Access:** Request access to personal data (Subject Access Requests, SARs).
- **Right to Rectification:** Correct inaccurate data, critical for SEN/SEMH records.
- **Right to Erasure:** Request deletion where lawful (e.g., non-essential data).
- **Right to Restrict Processing:** Limit processing in specific cases.
- **Right to Data Portability:** Obtain reusable data, where applicable.
- **Right to Object:** Object to processing based on legitimate interests or marketing.
- **Rights re Automated Decision-Making:** Not applicable, as we do not use automated decision-making.

SARs and rights requests are directed to the SEN Manager and responded to within one month, free of charge, unless complex. Requests from learners with SEN/SEMH are supported to ensure accessibility (e.g., assistance with forms).

10. Data Sharing

We share data only when necessary, with:

- **Department for Education (DfE):** For statutory reporting (e.g., SEN data, attendance).
- **Local Authorities:** For SEN/SEMH coordination or safeguarding.
- **Health/Social Services:** For learner welfare (e.g., CAMHS, medical needs).

- **Third-Party Processors:** IT systems or assessment platforms, under strict data processing agreements.

Sharing complies with UK GDPR, with agreements ensuring security. SEN/SEMH data is shared only with explicit justification, and parents/carers are informed via privacy notices, per DfE guidance.

11. Data Security

We implement robust measures to protect sensitive SEN/SEMH and staff data:

- **Technical Measures:** Encryption, secure servers, multi-factor authentication, and access controls.
- **Physical Measures:** Locked cabinets for paper records, restricted office access.
- **Organisational Measures:**
 - Annual staff training on data protection, with SEN/SEMH-specific modules.
 - Role-based access, limiting SEN/SEMH data to authorised staff (e.g., SENCO, mentors).
 - Regular security audits and penetration testing.

Devices are password-protected and encrypted. Portable devices carrying SEN/SEMH data are minimised and secured.

12. Data Retention

Data is retained only as long as necessary:

- **Learner Data:**
 - Safeguarding/SEMH records: Until the learner reaches age 25, per DfE safeguarding guidance.
 - SEN records (e.g., EHCPs): 7 years post-departure, unless required longer for legal reasons.
 - Educational records: 7 years post-departure, per DfE recommendations.
- **Staff Data:** 6 years post-employment for HR records, unless required longer (e.g., pension data).

Data is securely deleted or anonymised when no longer needed, following the DfE's disposal of records schedule.

13. Data Breaches

A data breach is any unauthorised or unlawful loss, access, or disclosure of personal data, particularly critical for SEN/SEMH data. Staff must report suspected breaches to the SEN Manager immediately. The SEN Manager will:

- Investigate and contain the breach within 24 hours.
- Notify the ICO within 72 hours if the breach poses a risk to individuals' rights.

- Inform affected data subjects (e.g., learners, parents/carers) if there's a high risk, using accessible formats.
- Document the breach, actions taken, and lessons learned.

Breaches involving SEN/SEMH data are prioritised due to their sensitivity.

14. Training

- **Staff:** Receive annual data protection training, including modules on handling SEN/SEMH data, breach reporting, and UK GDPR. New staff complete training during induction.
- **Learners:** Receive age-appropriate, SEN-accessible education on data privacy, integrated into online safety and SEMH workshops.
- **Parents/Carers:** Offered guidance on data rights and protecting learner information.

15. Third-Party Processors

Third parties (e.g., cloud providers, SEN assessment tools) must:

- Sign data processing agreements compliant with UK GDPR.
- Implement security measures matching our standards.
- Undergo regular compliance checks.

Data Protection Impact Assessments (DPIAs) are conducted for new systems handling SEN/SEMH data, per ICO guidance.

16. Monitoring and Review

- This policy is reviewed every year or following significant changes (e.g., new legislation, technology).
- The SEN Manager conducts annual audits to ensure compliance, focusing on SEN/SEMH data handling.
- Feedback from staff, learners, and parents/carers informs updates, with accessibility prioritised.

17. Consequences of Non-Compliance

- **Staff:** Face disciplinary action, up to dismissal, for breaches or failure to follow this policy.
- **Organisation:** Risks ICO fines, legal action, or reputational damage for non-compliance.
- Non-compliance undermines trust, particularly for vulnerable learners with SEN/SEMH needs.

18. Contact

For questions, concerns, or to exercise data subject rights:
SEN Manager

Email: laura.davis@bespokementoring.org

Phone: 07973778173

Address: Bespoke Mentoring and Training Services Limited, Regent Arcade, Newerne Street, Lydney, GL15 5RA

Complaints can be made to:

Information Commissioner's Office (ICO)

Website: www.ico.org.uk

Phone: 0303 123 1113

19. Related Policies

- Safeguarding Policy
- SEN Policy
- Anti-Bullying and Hate Crime Policy
- IT Acceptable Use Policy
- Behaviour and Learning Policy

Approval

This policy was approved by the Senior Leadership Team on April 28, 2025, and is effective immediately.

