

UNIQUE SEND TUITION

Data Protection Policy

Respectful, secure and transparent use of personal information

Data controller: Mandy Beadnell, trading as Unique SEND Tuition

Data protection contact: Mandy Beadnell - through the business contact details or website contact form

Effective from: September 2026

Review date: September 2027, and sooner following legal, technological or service changes

Version: 1.0

Personal information belongs to people, not to the business. Unique SEND Tuition will use only the information genuinely needed to provide safe, personalised tuition, meet legal and safeguarding responsibilities and run the service responsibly.

This policy explains how information is managed. A separate Privacy Notice will tell families, learners and other individuals what information is collected, why it is used, how long it is kept and how to exercise their rights.

1. Purpose and scope

This policy sets out the standards Unique SEND Tuition follows when collecting, using, recording, storing, sharing, transporting and deleting personal data. It applies to private tuition, EOTAS packages, agency or professionally referred work, home and community learning, outings, transport, enquiries, contracts, progress information, safeguarding, photographs, digital platforms and business administration.

Mandy Beadnell is a sole trader and is normally the data controller for private clients. For commissioned or agency work, the written agreement and actual use of the information will determine whether Unique SEND Tuition acts as an independent controller, joint controller or processor. Instructions that appear unlawful, unsafe or inconsistent with safeguarding duties will not be followed without clarification.

2. Legal framework

This policy is informed by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 where relevant, and amendments introduced by the Data (Use and Access) Act 2025 as they come into force. It is also read alongside safeguarding, contractual, financial and professional obligations.

Data protection law supports appropriate safeguarding information sharing. It does not require information to be withheld where sharing is necessary and proportionate to protect a child or another person.

3. Data protection principles

Lawfulness, fairness and transparency. Information will be used on a valid legal basis, in ways people can reasonably understand and expect.

Purpose limitation. Information will be collected for clear, legitimate purposes and will not be reused incompatibly.

Data minimisation. Only information that is adequate, relevant and necessary for the purpose will be collected or retained.

Accuracy. Reasonable steps will be taken to keep information accurate and to correct or clearly annotate disputed information.

Storage limitation. Information will not be kept in identifiable form for longer than necessary.

Integrity and confidentiality. Appropriate physical, organisational and technical safeguards will protect information from loss, misuse, alteration or unauthorised access.

Accountability. Decisions, lawful bases, sharing, retention and incidents will be recorded sufficiently to demonstrate responsible practice.

4. Information handled

Contact and identity information. Names, addresses, telephone numbers, email addresses, dates of birth and details of parents, carers and involved professionals.

Tuition and progress information. Starting points, learning needs, interests, targets, plans, attendance, observations, resources, progress summaries and professional correspondence.

Special category information. Health, disability, SEND, communication, behaviour, emotional wellbeing, ethnicity or other sensitive information where genuinely relevant to safe and effective provision.

Safeguarding and risk information. Concerns, disclosures, referrals, risk assessments, incident records, emergency information and proportionate details needed for outings or transport.

Business and financial information. Contracts, consent, fees, payment records, invoices and information needed for accounting, insurance or legal claims.

Images and digital information. Photographs, audio or video where separately agreed; website enquiries; platform account details; device, email and document metadata where relevant.

5. Lawful bases

A lawful basis will be identified before personal data is used and recorded where appropriate. The basis depends on the purpose and relationship, rather than convenience.

Contract. Processing necessary to respond to a requested service, arrange and deliver tuition, communicate about sessions and manage agreed payments or terms.

Legal obligation. Processing required for tax, accounting, safeguarding, court, regulatory or other applicable legal duties.

Legitimate interests. Necessary and proportionate administration, service improvement, security, professional liaison, record keeping or safeguarding activity, after considering the person's rights and reasonable expectations.

Vital interests. Processing needed in a genuine emergency to protect someone's life or physical safety.

Consent. Used where a genuine, informed and freely given choice is appropriate, particularly for optional uses such as specified photographs or marketing. Consent may be withdrawn for future use.

6. Special category and criminal offence data

Special category data requires both an Article 6 lawful basis and an additional Article 9 condition. Depending on the purpose, this may include explicit consent, vital interests, legal claims or substantial public interest conditions such as safeguarding children and individuals at risk. Any condition and supporting documentation required by law will be identified and retained.

Criminal offence information will be processed only where there is lawful authority and a clear need, for example in relation to safeguarding, suitability or legal proceedings. It will receive particularly careful access, sharing and retention controls.

7. Collecting information fairly

Information will normally be obtained directly from a parent, carer, learner or commissioning professional. Relevant information may also be received from schools, local authorities, agencies, health or care professionals and safeguarding services where there is an appropriate basis to share it.

People will be given an accessible Privacy Notice at the appropriate time. Explanations will be clear and proportionate to the learner's age, communication and understanding. A child's wishes and assent will be respected even where an adult provides legal consent.

8. Information security

Devices and accounts. Devices will use passwords or biometric protection, supported software, screen locking and appropriate security settings. Multi-factor authentication will be used where available for accounts holding sensitive data.

Storage. Electronic records will be stored in appropriately secured business systems. Paper records will be kept securely and out of view in homes, vehicles and community settings.

Transfer. Sensitive information will be shared through an agreed secure method. Recipient details and attachments will be checked before sending, and unnecessary forwarding or copying will be avoided.

Access. Access is limited to Mandy and to authorised recipients who require the information for a legitimate purpose. Personal information will not be discussed where it can be overheard.

Working away from a fixed base. Records and devices will not be left unattended in an unlocked vehicle or public place. Only the minimum necessary information will be taken to sessions, outings or meetings.

Back-up and recovery. Important records will be backed up using suitable secure arrangements, with reasonable steps taken to ensure availability and recovery after loss or technical failure.

9. Sharing information

Information may be shared with parents or carers, commissioning organisations, schools, local authorities, agencies, health and care professionals, insurers, accountants, legal advisers, safeguarding services, police or regulators where there is a valid purpose and lawful basis. Sharing will be relevant, necessary, proportionate and recorded when the context warrants it.

Consent will be sought where appropriate, but information may be shared without consent where this is necessary for safeguarding, preventing or detecting crime, complying with law or protecting vital interests. A decision not to share an important concern will also be reasoned and recorded.

10. Service providers and international transfers

Digital platforms, cloud storage, email, accounting, website, form and educational services may process information on behalf of Unique SEND Tuition. Providers will be selected with regard to privacy, security, contractual terms, access controls, deletion options and the amount of data required.

Where personal data is transferred outside the United Kingdom, an approved transfer mechanism and any necessary safeguards will be used. The location and privacy terms of a service will be checked before sensitive learner information is entered.

11. Photographs, recordings and website content

Photographs, video and audio will be created only for a clear agreed purpose, with appropriate written permission and regard to the learner's wishes. Permission for learning records does not automatically permit website, social-media or marketing use. Separate, specific permission is required for publication, and it may be withdrawn for future use.

Identifying details will be minimised. Images will not be stored indefinitely, used beyond the agreed purpose or taken on an unapproved personal device where a safer agreed method is available. Website images will normally use resources, licensed material or non-identifiable scenes rather than identifiable learners.

12. Artificial intelligence and automated tools

AI may be used to help create differentiated, age-appropriate and interest-led teaching resources. Names, contact details, photographs, case notes, medical details, safeguarding information, EHCP content or other information capable of identifying a learner will not be entered into public generative-AI tools.

AI output will be treated as a draft and checked by Mandy for accuracy, bias, accessibility, age appropriateness, copyright and safeguarding concerns. Significant decisions about a learner will not be made solely by an automated system. If future processing creates a high risk to people's rights, a Data Protection Impact Assessment will be completed before it begins.

13. Retention and secure disposal

A retention schedule will identify how long each category is kept, taking account of its purpose, contractual and tax requirements, safeguarding value, limitation periods, commissioning terms and the interests of the learner. Records subject to an active concern, complaint, claim, investigation or legal hold will not be destroyed until the matter and any required retention period have ended.

Routine enquiries. Unsuccessful or inactive enquiry information will normally be deleted when no longer needed, subject to a short period for follow-up and complaint handling.

Tuition and contractual records. Records will be reviewed when provision ends and retained only for the justified period recorded in the retention schedule.

Financial records. Invoices and accounting evidence will be retained for the period required by HMRC and other applicable legal obligations.

Safeguarding records. These will be kept separately and retained or transferred according to safeguarding need, local procedures, commissioning requirements and professional advice; they will not be routinely destroyed with teaching resources.

Paper will be cross-cut shredded or securely destroyed. Electronic records will be deleted from active storage and, where practicable, scheduled for removal from recycle bins, synchronised devices and back-ups in line with provider arrangements.

14. Individual rights and requests

Depending on the circumstances, individuals may have rights to be informed; access their information; request correction or erasure; restrict or object to processing; receive portable data; and receive safeguards relating to automated decision-making. Some rights are qualified and may not override safeguarding, legal or third-party rights.

Requests may be made verbally or in writing and should be passed promptly to Mandy. Identity and authority may be checked proportionately. Reasonable and proportionate searches will be made, and the statutory response period will be followed. Where clarification is genuinely needed, the request will be handled in accordance with the current rules on pausing the response period.

15. Children's rights and parental access

Data protection rights belong to the child as well as to adults. A parent or carer does not automatically have an unrestricted right to every record. The learner's age, understanding, competence, best interests, confidentiality, safeguarding, court orders and the rights of other people will be considered before information is disclosed.

Information intended for learners will be explained in accessible language and format. Where a learner can understand and exercise their own rights, their request and wishes will be given appropriate weight.

16. Personal data breaches

A suspected loss, misdirection, unauthorised disclosure, cyber incident or inappropriate access must be contained and assessed immediately. Delay can increase harm.

Contain and recover. Secure accounts or devices, recall or request deletion of information, preserve evidence and take proportionate steps to limit further exposure.

Record. Document what happened, when it was discovered, the information and people affected, likely consequences, actions taken and the reasoning behind notification decisions.

Assess risk. Consider the sensitivity, volume, identifiability, recipients, vulnerability of the individuals and possible physical, emotional, financial, reputational or safeguarding harm.

Notify where required. A breach likely to risk people's rights and freedoms will be reported to the ICO without undue delay and, where feasible, within 72 hours of awareness. A high-risk breach will also be communicated to affected individuals without undue delay, unless a lawful exception applies.

Safeguarding. If a breach may place a child at risk, the Safeguarding & Child Protection Policy will be followed alongside the data breach response.

17. Concerns, complaints and ICO contact

A person concerned about how their information has been handled should contact Mandy using the business contact details or website form. The concern will be acknowledged, investigated fairly, and answered with the outcome and any action taken. The Complaints Policy may also be used.

Individuals may complain to the Information Commissioner's Office (ICO) through its official website or by telephone on 0303 123 1113. Raising a concern with Unique SEND Tuition first may allow it to be resolved promptly, but this does not remove the right to contact the ICO.

18. Accountability and review

Mandy will maintain proportionate records of processing, lawful bases, consent where used, retention decisions, processors, information sharing, rights requests, breaches and Data Protection Impact Assessments where needed. Data protection considerations will be included when introducing new services, forms, digital platforms or working arrangements.

This policy will be reviewed at least annually and sooner after a data incident, complaint, material change in processing, new technology or relevant change in law or ICO guidance. The Privacy Notice, consent wording, retention schedule and supplier arrangements will be reviewed alongside it.

Nurture • Explore • Grow