Data Protection Policy and Privacy Notice

EmpowerEd North Ltd | Data Protection Lead: Janice March, Founder and Director

Version 1.3 | Revised: 3 November 2026 | Scheduled review: 3 November 2027, or sooner following a relevant change, breach or concern

Contact: admin@empowered-north.co.uk | www.empowered-north.co.uk

Part A: Privacy notice

1. Who is responsible

EmpowerEd North Ltd, trading as EmpowerEd North, is responsible as controller for the personal information it uses to run its own education and support services. The Data Protection Lead can be contacted at admin@empowered-north.co.uk. ICO registration reference: CSN6634187.

Where a school or local authority commissions support, its responsibilities and EmpowerEd North's controller or processor role will be agreed for the actual processing. A commissioning contract does not automatically make EmpowerEd North a processor or give it the commissioner's statutory powers.

2. What we collect and where it comes from

We collect information necessary for enquiries, tuition, commissioned support, outreach, sensory stories and business administration. Depending on the service, this can include learner and adult contact details; emergency contacts; subjects and learning needs; education and EHCP information; communication, sensory, disability and health information; attendance and progress; risk assessments; safeguarding and incident records; authorised photographs; booking and payment information; correspondence; and relevant workforce and recruitment records.

Information comes from the person concerned, parents or carers, referrers, schools, local authorities and other professionals; from our teaching and observations; and from relevant checks or agencies. We do not require every category for every service. Please avoid sending complete medical or EHCP records through an initial general enquiry. We will agree a suitable route where sensitive information is needed.

3. Why we use information and our lawful bases

For each purpose, we identify the actual lawful basis before processing. These are the bases used where their conditions apply:

- Enquiries and bookings: taking requested steps towards a contract or performing a contract with the person concerned; legitimate interests in responding to a parent or professional where the learner is not the contracting person.
- Teaching, support, progress reporting and safe delivery: contract where the person concerned is a party; otherwise legitimate interests in providing suitable education, communicating and managing the service, balanced against the individual's rights. We identify any separate legal duty where it applies.
- Safeguarding and necessary welfare sharing: the applicable legal obligation, including the information-sharing duty where within scope, or legitimate interests where appropriate. Vital interests is reserved for circumstances meeting that legal test, rather than used as a general basis for routine care.
- Invoices, tax, insurance, complaints and legal matters: contract, applicable legal obligations and legitimate interests in accurate administration, resolving concerns and establishing or defending claims.
- Recruitment and employment: steps towards or performance of a contract, legal obligations and legitimate interests in fair recruitment and safe staffing, according to the particular record and role.

- Optional publicity: specific consent, which can be withdrawn. Refusing consent does not affect access to education or support.

We do not automatically rely on public task because a public body pays for provision. Any reliance requires an identified task with a basis in law. Where legitimate interests is used, we assess necessity, the individual's reasonable expectations and the impact on their rights, especially for children.

Health, disability and some other information have extra protection. We need an Article 6 basis and a separate Article 9 condition. For routine optional health or SEND information necessary to tailor privately arranged support, we use explicit, informed consent where appropriate; explain what is needed and why; and review safe service options if consent is withdrawn. For safeguarding, substantial public interest and the Data Protection Act 2018 Schedule 1 safeguarding condition may apply where all its requirements are met. Employment-related information and legal claims use the relevant separate conditions where applicable. Each special-category condition is assessed against the purpose and circumstances of the processing. Criminal-offence and DBS information requires the applicable Article 10 authority and domestic-law safeguards.

4. Who receives information

We share relevant information only where lawful and necessary: with the learner and authorised parents or carers; placing schools, colleges and commissioners; professionals involved in support; social care, safeguarding agencies, LADO and police; courts, regulators or DBS where required; and insurers, legal/accounting advisers and service suppliers where needed.

For adults, parents are not automatically entitled to records. For children, we consider understanding, confidentiality, parental authority and safeguarding. We explain sharing unless doing so would increase risk, prejudice an investigation or be otherwise inappropriate under the law. Necessary safeguarding sharing may take place without consent and before a situation becomes an emergency.

Approved IT, email, hosting, storage and administration suppliers may process information under appropriate contracts and access restrictions. We assess supplier roles, security, retention and international transfers before use. Transfers outside the UK require an applicable adequacy arrangement or other lawful safeguards and any required risk assessment. Contact the Data Protection Lead for information about safeguards relevant to your data. We do not sell personal information.

5. Retention

We retain information only for a justified purpose. The following retention and review periods apply, subject to relevant legal requirements and documented exceptions. A documented safeguarding, investigation, complaint, insurance or legal hold overrides routine deletion. The Data Protection Lead records reasons for exceptions and reviews them.

- General enquiries that do not become a service: delete 12 months after last meaningful contact unless a documented reason requires longer.
- Substantive referrals that do not proceed: review after 12 months; normally delete within three years of the decision unless a specific safeguarding, contractual or legal reason supports longer.
- Routine teaching, progress and booking records: normally six years after the service ends, or return/transfer under the agreed commissioner arrangement. Remove duplicate working copies sooner. Separate significant safeguarding, medical and injury records from routine disposal.
- Child safeguarding records: normally retain until the learner's 25th birthday, with longer retention where needed for an investigation, claim, inquiry or applicable requirement. Agree secure transfer and responsibility with the receiving organisation. Do not erase EmpowerEd North's necessary accountability record simply because a summary was transferred.
- Adult safeguarding records: review at case closure and annually thereafter; a six-year baseline after closure applies unless the authority, insurer or legal circumstances justify a different period. Do not dispose while risk

or proceedings remain unresolved.

- Significant accident, medical, medication and restraint records: for children, normally retain until age 25; for adults, normally six years after the incident or end of relevant support, whichever is later. Check insurer, safeguarding and legal requirements before disposal. Keep required RIDDOR records for at least three years from the record date.
- Harm-threshold allegations about adults working with children: follow current safeguarding guidance, normally until normal pension age or ten years from the allegation, whichever is longer. Apply the guidance's specific exceptions, including malicious or false allegations, rather than retaining every allegation indiscriminately. Obtain advice before disposal.
- Low-level concerns: retain at least for the engagement; review at departure. Retain longer only where justified by patterns, safeguarding, employment or legal need, with a recorded review date.
- Unsuccessful recruitment: normally six months after the decision. Employment records: normally six years after employment ends, separating records with different statutory or safeguarding periods. DBS certificate copies are normally kept no longer than six months; retain a permitted check record rather than an unnecessary certificate copy.
- Finance and tax records: normally six years from the end of the relevant accounting year, or longer where applicable accounting/tax rules require.
- Complaint and data-breach records: normally six years after closure, retaining only necessary information; separate safeguarding records may need longer.
- Publicity images: review need and permissions at least annually, remove when no longer needed or consent is withdrawn where we control the publication, and retain necessary permission/withdrawal evidence for up to six years after last use to demonstrate compliance.
- Website enquiry copies: remove duplicate form or inbox copies once transferred to the appropriate record and no longer needed. Visitor/attendance information for events: normally 12 months unless needed for finance, an incident, safeguarding or a documented service purpose.

6. Your rights and requests

Depending on the processing, you may request access, correction, erasure, restriction or portability, object to processing, or withdraw consent. Rights have limits: for example, a safeguarding or legal record may need to be retained after a request to delete it. Withdrawal does not make earlier lawful use unlawful. We do not use solely automated decisions with legal or similarly significant effects about learners.

Contact the Data Protection Lead verbally, by email or through an accessible method. You do not need special wording. We normally respond within one month under the applicable rules, explain any lawful extension within the original period, and provide reasons and complaint rights if declining a request. Identity or authority checks will be proportionate. A parent's access request is assessed in light of the child's understanding, rights and safety; parental status alone does not determine every request.

7. Concerns and complaints

Contact admin@empowered-north.co.uk. We aim to acknowledge within five working days and will meet the statutory 30-day acknowledgement deadline, calculated under the applicable rules. We investigate without undue delay, keep you informed and explain the outcome. A complaint and a rights request have separate legal timetables. You may complain to the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/.

8. Website, cookies and communications

Website enquiries are made by email. Please provide only the information needed for an initial response; detailed health, safeguarding and EHCP records should be shared through an agreed route. Business email and related administration use Microsoft services. Service-specific forms provide additional information about the data requested and its purpose.

Cloudflare hosts and protects this website and may process technical information such as IP address, request time and browser details for delivery, security and performance. The website also includes Cloudflare Web Analytics. Google Analytics is optional and is loaded only after a visitor accepts analytics through the cookie controls. It helps us understand visits and page use. These suppliers may process data internationally under their applicable transfer safeguards. Further information is available in the Cloudflare privacy policy (https://www.cloudflare.com/privacypolicy/), Microsoft privacy statement (https://privacy.microsoft.com/privacystatement) and Google privacy policy (https://policies.google.com/privacy).

The browser stores the analytics preference under empoweredNorthAnalyticsConsent until it is changed or browser storage is cleared. Visitors can accept or decline optional analytics and change their choice using Cookie settings. Declining does not prevent use of the website. Google Analytics may use _ga cookies to distinguish visits; their standard lifetime is up to two years, and browser controls can remove them sooner. Contact the Data Protection Lead for information about retention and safeguards applying to particular records.

External booking, form and social-media links lead to services with their own privacy information. Marketing communications must meet applicable data-protection and electronic-marketing requirements and provide a simple opt-out.

9. Short explanation for learners

We keep some information to help us teach you, understand your communication and support you safely. We keep it private and share it only with people who need it for a lawful reason. Sometimes we must tell someone if we are worried about safety. You can ask the Data Protection Lead what information we keep, ask for help to understand it, or tell us if something is wrong. We can explain using your preferred communication.

Part B: Data protection responsibilities and procedures

10. Accountability, collection and access

The Data Protection Lead keeps a proportionate record of processing purposes, lawful bases, special-category conditions, supplier roles, recipients, security and retention. Keep an appropriate policy document where required for the condition used under the Data Protection Act. Before new high-risk processing, complete a data-protection impact assessment and resolve unacceptable risks.

Collect the minimum necessary, keep information accurate and correct errors promptly. Use role-based access, strong unique passwords, multi-factor authentication where available, secure devices, updates, encrypted storage/transfers where appropriate, and locked paper storage. Keep safeguarding records apart from routine teaching files. Do not leave records visible in homes, cars or community venues. Confidentiality continues after a person's engagement ends.

A personally owned device used for business must be approved, secured and separated from personal accounts/backups and family access as far as practicable. No unapproved cloud, messaging or AI systems may hold identifiable learner information. De-identification must consider indirect identification through detailed circumstances, not just removal of names.

11. Sharing and suppliers

Verify recipients and their authority, use secure transfer, share the minimum and record significant safeguarding sharing decisions. Agree controller/processor roles and applicable processor contracts or sharing arrangements. Do not assume the commissioner's lawful basis automatically becomes EmpowerEd North's basis. Check storage, onward transfers, sub-processors, deletion and breach notification before authorising a supplier. Give clear additional privacy information if a new use materially changes this notice.

12. Breaches and security incidents

Report any lost file/device, wrong-recipient message, unauthorised access, accidental disclosure, damaging deletion or other suspected breach to the Data Protection Lead immediately. Contain the incident safely, preserve necessary evidence, assess harm and record the decision and remedial action. If the Data Protection Lead is unavailable, staff must take appropriate immediate containment action and obtain supplier or professional assistance. Statutory reporting deadlines continue to apply.

Notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk people's rights and freedoms. Record reasons for reporting or not reporting and explain any delay. Tell affected individuals without undue delay where high risk requires it, subject to lawful exceptions. A processor must inform the controller without undue delay. Refer any associated safeguarding concern through the safeguarding route immediately.

13. Review and disposal

Those with access to personal information receive induction and relevant updates at least annually and when systems or law change. The Data Protection Lead reviews access, suppliers, retention, permissions, complaints and incidents at least annually. Dispose securely, including unnecessary working copies, and manage backups through documented deletion cycles and restricted restoration. Do not alter or destroy information to frustrate a rights request, complaint or investigation.

Main reference points: UK GDPR; Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025; applicable Privacy and Electronic Communications Regulations; current ICO guidance; safeguarding legislation and September 2026 information-sharing guidance. Read with the Safeguarding, Online Safety and Complaints policies.