Data Protection Policy and Privacy Notice

EmpowerEd North policy suite

This policy has been adopted for use from May 2026 and should be reviewed against current legal, safeguarding, commissioning, website and operational arrangements at least annually and whenever guidance or operational arrangements change.

Policy information	Details
Date adopted	May 2026
Review date	May 2027, or sooner following a review trigger listed in this policy
Approved by	EmpowerEd North Founder/Director
Named lead	Data Protection Lead - Janice March
Version	1.0
Owner/responsible person	Data Protection Lead / EmpowerEd North Founder/Director
Completion status	CURRENT - adopted for use from May 2026. Operational evidence and contact sheets must be kept up to date before each placement.
Operational arrangements	Confirm Data Protection Lead; ICO registration/data protection fee position; data retention schedule; approved systems; processor arrangements; data-sharing arrangements with commissioners; consent forms; website privacy notice; breach response route.

Immediate data protection action box

Situation	Required action
Possible personal data breach	Tell the Data Protection Lead immediately. Preserve evidence. Do not delete, edit, hide or forward material unless instructed to secure it. The Data Protection Lead must assess whether the ICO and/or affected people must be informed. Serious breaches may need ICO reporting within 72 hours of EmpowerEd North becoming aware.
Safeguarding concern	Safeguarding overrides routine confidentiality where a child, young person or adult at risk may be at risk of harm. Report immediately to the DSL and follow the Safeguarding Policy. Record what was shared, with whom, why and when.
Subject access request or request for information	Forward immediately to the Data Protection Lead. Requests may be written, verbal, informal or sent by email. Do not ignore requests because they do not use the phrase "subject access request".
Request to delete or change information	Forward to the Data Protection Lead. Do not delete records

	needed for safeguarding, legal, contractual, regulatory, education, complaint or insurance purposes without authorised review.
Use of a new app, system, AI tool, cloud storage, camera or communication channel	Do not use with learner, family, staff or safeguarding information until it has been approved, risk assessed and added to the Approved Systems Register where required.

1. Purpose

EmpowerEd North is committed to protecting personal information and handling it lawfully, fairly, transparently and securely. This policy explains how EmpowerEd North collects, uses, stores, shares, retains and disposes of personal data relating to learners, parents/carers, staff, volunteers, contractors, visitors, commissioners and professional partners.

The policy is designed for a small specialist SEND alternative provision operating from a main base, community venues, off-site locations, home/community-based support and digital systems. It should be read alongside the Privacy Notice in Part Two of this document.

2. Scope

This policy applies to:

- all EmpowerEd North directors, staff, volunteers, agency staff, contractors, self-employed workers, visiting professionals and anyone working with or on behalf of EmpowerEd North;
- all personal data processed by EmpowerEd North, including learner, parent/carer, staff, visitor, contractor, referrer, commissioner and professional information;
- all formats and locations, including paper files, electronic records, email, cloud storage, mobile devices, laptops, tablets, photographs, video, audio, CCTV if ever used, website enquiries and online learning systems;
- all delivery models, including premises-based, community-based, off-site, home/community support and remote or digital activity.

3. Legal and guidance framework

This policy is informed by:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;

Data (Use and Access) Act 2025, where relevant to current and forthcoming changes to UK data protection and privacy law;

- Privacy and Electronic Communications Regulations (PECR), where relevant to electronic communication and marketing;
- Information Commissioner's Office (ICO) guidance, including guidance on lawful basis, special category data, individual rights, subject access requests, data sharing, data security, personal data breaches and children's information;
- DfE data protection guidance for schools and education settings, where relevant and useful to alternative provision practice;
- Keeping Children Safe in Education (KCSIE) 2025, where relevant to safeguarding records, information sharing and safer recruitment;
- Working Together to Safeguard Children 2026, where relevant to safeguarding information sharing;
- Alternative provision statutory guidance, Department for Education, last updated 5 February 2025, where relevant to commissioner information-sharing arrangements;

DfE non-school alternative provision (AP) voluntary national standards, published August 2025, where relevant to commissioner expectations, safeguarding records and information sharing;

- Equality Act 2010, SEND Code of Practice: 0 to 25 years, and safeguarding partnership procedures, where relevant.

4. Data protection principles

EmpowerEd North will process personal data in line with the UK GDPR principles. Personal data must be:

Principle	What this means for EmpowerEd North
Lawful, fair and transparent	Individuals should understand why their information is being collected and how it will be used, unless there is a lawful reason not to tell them immediately, such as safeguarding or crime prevention.
Purpose limited	Information should be collected for specified, explicit and legitimate purposes and not used in ways that are incompatible with those purposes.
Data minimised	Only information that is relevant and necessary should be collected or shared.
Accurate and up to date	Records should be factual, attributable, dated and corrected where appropriate. Professional judgement should be clearly distinguished from fact.
Storage limited	Information should not be kept for longer than necessary. Retention should follow the Data Retention Schedule unless a lawful reason requires longer retention.
Secure and confidential	Information must be protected against unauthorised access, accidental loss, destruction or damage.
Accountable	EmpowerEd North must be able to show how it complies with data protection requirements.

5. Data controller, processor and commissioning roles

EmpowerEd North will usually act as a data controller for the personal data it collects and uses to manage enquiries, admissions, learner support, safeguarding, staffing, finance, complaints, governance and business operations.

Where a learner is placed or commissioned by a school, college, local authority or other organisation, data protection roles must be clarified before the placement begins. Depending on the arrangement, EmpowerEd North may be an independent controller, a joint controller, or a processor for specific activities. This must be recorded in the placement agreement or data-sharing/processing arrangement.

EmpowerEd North must not assume that a commissioner's data protection arrangements cover EmpowerEd North's own records, systems, devices, website, email accounts or safeguarding records. Where uncertainty exists, the Data Protection Lead must seek advice and record the decision.

6. Roles and responsibilities

Role	Responsibilities
Founder/Director	Overall accountability for ensuring appropriate data protection governance, resources, systems, training, records and review.
Data Protection Lead	Day-to-day lead for data protection compliance; privacy notices; record of processing; breach response; subject access requests; retention schedule; processor and data-sharing checks; liaison with the ICO where required. Name: Janice March.
Designated Safeguarding Lead	Ensures safeguarding information is shared lawfully, proportionately and promptly where risk of harm is present. Works with the Data Protection Lead where safeguarding and data protection overlap.
All staff, volunteers and contractors	Follow this policy; protect information; use approved systems; report breaches and near misses immediately; complete training; and ask for advice where unsure.
Commissioners / placing schools / local authorities	Agree information-sharing, attendance, safeguarding, reporting and record-transfer routes before placement starts.
Data processors / suppliers	Process personal data only as agreed with EmpowerEd North and with appropriate contractual, technical and organisational safeguards.

7. Types of personal data processed

EmpowerEd North may collect and process the following categories of information where relevant and necessary:

Category	Examples
Learner information	Name, date of birth, address, contact details, emergency contacts, school/commissioner details, EHCP information, attendance, timetable, learning records, progress records, behaviour support, risk assessments, communication profiles, sensory profiles, medical information, medication information, incident records, first aid records, transport information, photographs/video where authorised, and views/voice of the learner.
Special category data	Health, disability, SEND, sensory needs, communication needs, ethnicity where relevant, safeguarding information, and other sensitive information needed for support, safety, equality, statutory or safeguarding purposes.
Safeguarding and welfare records	Concern forms, chronologies, referrals, agency communications, risk assessments, body maps, child-on-child abuse records, allegations/low-level concern links, online safety records, attendance safeguarding concerns and information from external professionals.
Parent/carer/family information	Names, contact details, relationship to learner, parental responsibility information where needed, communication records, family context where relevant to support or safeguarding, and consent/permission records.
Staff, volunteer and contractor data	Recruitment records, identity/right to work checks, DBS/check evidence, references, training, supervision, payroll/payment information, next-of-kin, absence, conduct, safeguarding allegations and low-level concern records where relevant.
Visitor and professional partner data	Names, organisation, contact details, visit logs, identity checks, meeting notes and correspondence.
Digital and technical data	Email records, system audit logs, device identifiers, approved platform use, website enquiry data, online safety incident records and cyber security records.
Images, video, audio and CCTV	Photographs, video, audio or CCTV only where there is a clear lawful basis, safeguarding/premises reason, consent where required, and approved storage arrangements. CCTV is not assumed to be in use.
Financial and contractual data	Invoices, payment details, funding/commissioning records, contracts, insurance records and supplier information.

8. Lawful bases for processing

EmpowerEd North will identify and record an appropriate lawful basis before processing personal data. More than one lawful basis may apply to different parts of a learner, staff or business record.

Lawful basis	How it may apply
Contract	Used where processing is necessary to provide a service, manage a placement agreement, employ staff, engage contractors or administer fees.
Legal obligation	Used where EmpowerEd North must meet legal requirements, including safeguarding, employment, tax, health and safety, statutory record-keeping or regulatory obligations.
Vital interests	Used where processing is necessary to protect someone's life or immediate safety, for example a medical emergency.
Legitimate interests	Used where EmpowerEd North has a legitimate business, education, safeguarding, operational or safety interest and this does not override the rights and freedoms of the individual. A balancing assessment should be recorded where appropriate.
Public task / official authority	May apply where EmpowerEd North is carrying out a task in the public interest or exercising official authority through a school/local authority commissioned arrangement. This must not be assumed and should be clarified in commissioner agreements.
Consent	Used for genuinely optional processing, such as some publicity images, optional testimonials, non-essential communications or certain optional activities. Consent must be specific, informed, freely given and capable of being withdrawn.

9. Special category and criminal offence data

EmpowerEd North will often need to process special category data because many learners have SEND, health, sensory, communication, medical, safeguarding or welfare needs. This must be handled with particular care.

When processing special category data, EmpowerEd North must identify both a UK GDPR Article 6 lawful basis and a relevant Article 9 condition. Depending on the context, this may include explicit consent, employment/social protection obligations, vital interests, health or social care purposes, safeguarding of children or individuals at risk, equality monitoring, or substantial public interest conditions set out in the Data Protection Act 2018.

Criminal offence data, including allegations, police involvement, youth justice information or offence-related safeguarding information, must only be processed where lawful and necessary, with an appropriate condition under the Data Protection Act 2018 and restricted access.

10. Collecting information

Information may be collected from learners, parents/carers, schools, local authorities, health professionals, social care, previous settings, referral forms, EHCPs, assessments, meetings, emails, phone calls, safeguarding records, incident records and direct observation.

Information collection must be purposeful and proportionate. Staff should avoid collecting information simply because it might be useful later. Where information is sensitive, staff must be clear why it is needed, who will access it and how it will be stored.

11. Privacy notices and transparency

EmpowerEd North will make privacy information available to learners, parents/carers, staff, volunteers, contractors and website users. Privacy information should be accessible and understandable. Where learners have communication needs, information should be adapted where appropriate using plain English, visuals, discussion, AAC or a trusted adult to support understanding.

Privacy information must explain what data is collected, why it is used, the lawful basis, who it may be shared with, how long it is kept, rights of individuals, how to complain and how to contact EmpowerEd North. Part Two of this document contains the main Privacy Notice.

Where information is collected through the website, online forms, digital tools, AI tools, social media, mailing lists, photographs/video or CCTV if ever used, the relevant privacy information must be available before or at the time information is collected wherever practicable.

12. Information sharing

EmpowerEd North will share personal data where lawful, necessary and proportionate. Safeguarding information must be shared promptly where a child, young person or adult at risk may be at risk of harm. Data protection law must not be used as a reason to delay or avoid appropriate safeguarding information sharing.

Information may be shared with placing schools, colleges, local authorities, children's social care, adult safeguarding, health professionals, police, safeguarding partnerships, LADO, DBS, courts, insurers, legal advisers, payroll/accounting providers, IT providers, approved digital systems and regulators where relevant and lawful.

Before routine or planned sharing, staff should consider:

- what information needs to be shared and why;
- the lawful basis and any special category condition;
- whether the individual should be informed, unless this would increase risk or undermine safeguarding/legal action;

- whether the information is accurate, relevant, necessary and proportionate;
- how it will be shared securely;
- whether a data-sharing agreement or commissioner protocol is needed;
- what record should be made of the sharing decision.

13. Consent

Consent will only be used where the individual has a genuine choice and the processing is optional. Consent is not usually the right lawful basis where EmpowerEd North must process information for safeguarding, legal obligation, contractual provision, health and safety, employment or commissioned education purposes.

Consent forms must be specific. A broad consent form for "everything" is not sufficient. Separate decisions should be recorded for publicity images, use of photographs/video for internal learning records, off-site permissions, information sharing where consent is appropriate, and any optional digital or marketing activity.

Where a learner may have capacity to make their own decision, EmpowerEd North will consider age, understanding, communication needs and the nature of the decision. For learners aged 18 or over, consent and capacity must be considered in line with adult safeguarding and Mental Capacity Act principles where relevant.

14. Learner voice, communication and SEND accessibility

Data protection practice must be accessible to learners with autism, severe learning disabilities, communication differences, sensory needs and anxiety. Staff must support learners to understand, as far as reasonably possible, what information is being recorded about them, how it may be used and who they can speak to if they are worried.

Learners may communicate through speech, AAC, gesture, behaviour, signs, objects, visuals, drawing, writing or body language. Records must not misrepresent a learner's communication. Where staff interpret behaviour or communication, the record must distinguish what was observed from professional interpretation.

15. Records and record quality

Records must be accurate, factual, dated, attributable and written in professional language. They must distinguish between fact, direct observation, professional judgement and information reported by others.

Records should be sufficient to explain decisions, actions, risk management and follow-up. They should not include unnecessary personal opinion, irrelevant family detail, discriminatory language, speculation presented as fact, or excessive information not needed for the purpose.

16. Security and confidentiality

EmpowerEd North will protect personal data through appropriate technical and organisational measures. These will include, as relevant:

- secure passwords and multi-factor authentication where available;
- restricted access to learner, safeguarding, staff and finance records;
- approved cloud storage and email accounts only;
- clear separation of personal and work devices/accounts;
- encryption or secure transfer for sensitive files where appropriate;
- locked storage for paper records;
- clear desk and secure disposal arrangements;
- regular backup and recovery arrangements;
- device locking and secure screen practices;
- confidential conversations held in appropriate places;
- staff training and supervision;
- prompt reporting of suspected breaches or near misses.

17. Approved systems, devices and AI tools

Only approved systems, devices, email accounts, cloud storage, messaging routes and digital tools may be used for EmpowerEd North personal data. The Data Protection Lead will maintain an Approved Systems Register.

Staff must not upload learner, family, staff, safeguarding, medical, EHCP, behaviour, incident, image, video or confidential business information into unapproved apps, public AI tools, personal email, personal cloud storage or personal messaging accounts.

Before using any AI tool with personal data, EmpowerEd North must complete a risk assessment covering privacy notice information, lawful basis, data minimisation, security, retention, provider terms, overseas transfer, accuracy, safeguarding risk, human review and whether the tool uses inputs for training.

18. Photographs, video, audio and publicity

Images, video and audio recordings can be highly sensitive, particularly for learners with SEND. EmpowerEd North will separate the purposes for which images or recordings may be used:

Use	Control required
Internal learning/support records	May be used where necessary and lawful to evidence progress, communication, behaviour support, risk assessment, EHCP outcomes or safeguarding/incident follow-up. Access must be restricted and records retained according to

	purpose.
Publicity, website or social media	Requires clear, specific consent. Consent must identify where images may appear and must be capable of withdrawal for future use. Extra care is required for vulnerable learners and safeguarding situations.
Safeguarding or incident evidence	May be processed where necessary for safeguarding, legal obligation, vital interests or substantial public interest. Do not publish. Restrict access and store securely.
CCTV	Not assumed to be in use. If introduced, EmpowerEd North must complete a DPIA, display appropriate signage, update privacy information and define access, retention and review arrangements before activation.

19. Data processors, suppliers and overseas transfers

Before using a supplier or digital service that processes personal data for EmpowerEd North, the Data Protection Lead must check whether a written processor agreement, contract terms, data-processing addendum or data-sharing agreement is required.

Supplier checks should include what data is processed, where it is stored, whether data is transferred outside the UK, security measures, retention/deletion arrangements, sub-processors, breach notification requirements and whether information may be used for the supplier's own purposes.

Overseas transfers must only take place where lawful safeguards are in place, such as adequacy regulations or appropriate contractual safeguards. This must be checked before using systems that store or process data outside the UK.

20. Data protection impact assessments

A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in high risk to individuals. Examples may include:

- new systems processing learner, safeguarding, medical or SEND data;
- CCTV, audio recording, monitoring technology or location tracking;
- use of AI tools with personal data;
- new online learning, communication or case-management platforms;
- systematic monitoring or profiling;
- large-scale or high-risk special category data;
- new information-sharing arrangements with commissioners or external providers;
- any processing involving particularly vulnerable learners where risk is increased.

21. Individual rights

Individuals may have rights to be informed, access their data, request rectification, erasure, restriction, objection, portability and rights relating to automated decision-making. These rights are not absolute and may be limited by safeguarding, legal, employment, contractual or record-keeping requirements.

Requests may be made verbally or in writing and must be forwarded immediately to the Data Protection Lead. EmpowerEd North will verify identity where necessary and respond within statutory timescales. Staff must not delete, alter or withhold records because a request has been made.

22. Subject access requests

A subject access request (SAR) is a request by an individual for access to their personal data. Staff must recognise that a SAR does not need to use technical language. Examples include "Can I see what you hold about me?" or "Please send me my child's records".

The Data Protection Lead will coordinate SAR responses, including identity checks, scope clarification, searches, third-party redactions, safeguarding review, exemptions where relevant and secure disclosure.

Requests for a child's information must be considered carefully. Parental responsibility, the child's age and understanding, best interests, safeguarding risk, confidentiality of third parties and the nature of the records must all be considered.

23. Data breaches and near misses

A personal data breach is a security incident affecting personal data. It may involve accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include sending information to the wrong person, losing a device or paper file, unauthorised access to a learner file, cyber attack, leaving confidential records visible, loss of a USB stick, accidental deletion, sharing photographs without authority or using an unapproved system.

All suspected breaches and near misses must be reported to the Data Protection Lead immediately. The Data Protection Lead will assess risk, contain the breach, record the incident, decide whether ICO notification is required, decide whether affected individuals must be told, and identify learning actions. Where a breach creates safeguarding risk, the DSL must also be informed immediately.

24. Retention and disposal

EmpowerEd North will maintain a Data Retention Schedule. Records must not be kept indefinitely without reason, but must not be destroyed where they may be needed for safeguarding, allegations, complaints, legal claims, insurance, commissioner audit, employment, finance or regulatory purposes.

Secure disposal must be used for paper and electronic records. Deletion must include reasonable steps to remove files from live systems, shared folders and devices. Disposal decisions for safeguarding, allegation, medical, employment and complaint records must be authorised by the Data Protection Lead and/or DSL as appropriate.

25. Staff training and confidentiality

All staff, volunteers and contractors with access to personal data will receive data protection, confidentiality and information security induction before accessing learner or family records. Refresher training will be completed at least annually or sooner where systems, law, risk or roles change.

Confidentiality obligations continue after employment, volunteering, contract or placement ends.

26. Website, enquiries and electronic communications

EmpowerEd North will ensure that website enquiry forms, contact forms and email communications are supported by appropriate privacy information. Website forms should collect only necessary information and should not invite unnecessary sensitive information unless the form is secure and the purpose is clear.

Marketing or general updates will only be sent where there is a lawful basis and any PECR requirements are met. Individuals must be able to opt out of non-essential communications.

27. Monitoring, audit and review

The Data Protection Lead will monitor implementation of this policy through review of breach records, subject access requests, consent records, processor arrangements, approved systems, retention checks, training records, data-sharing decisions and commissioner requirements.

This policy will be reviewed annually and sooner where law, ICO guidance, DfE guidance, systems, venues, operating model, staffing, commissioner requirements, breach learning or safeguarding arrangements change.

28. Linked policies and templates

- Safeguarding, Child Protection and Safer Recruitment Policy
- Managing Allegations and Low-Level Concerns Policy
- Online Safety Policy

- Staff Code of Conduct and Safer Working Practice Policy
- Behaviour Support Policy
- Attendance and Absence Policy
- First Aid Policy
- Health and Safety Policy
- Complaints Policy
- Whistleblowing Policy
- Staff Mobile Phone, Devices, Images and Social Media Policy
- Risk Assessment Policy
- Lone Working Policy
- Educational Visits and Community Learning Policy
- Data Retention Schedule
- Approved Systems Register
- Data Breach Record
- Subject Access Request Log
- Consent Forms
- Data Sharing Decision Record
- Processor / Supplier Due Diligence Checklist

Part Two: Privacy Notice

This Privacy Notice explains how EmpowerEd North collects and uses personal information. It should be made available to learners, parents/carers, staff, volunteers, contractors, commissioners and website users as relevant. A shorter learner-friendly version is included after the main notice.

1. Who we are

EmpowerEd North provides specialist part-time alternative provision and individualised education support for children and young people with SEND, including autism, severe learning disabilities, communication needs, sensory needs and complex support needs.

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

Data Protection Lead: Janice March

2. What information we collect

We may collect information about learners, parents/carers, staff, volunteers, contractors, visitors, commissioners and professional partners. This may include contact details, education records, EHCP information, attendance, progress, communication needs, sensory needs, health and medical information, behaviour support, risk assessments, safeguarding records, incident and first aid records, images/video where authorised, staffing records, recruitment checks, payment information and correspondence.

3. Why we use personal information

We use personal information to:

- respond to enquiries and referrals;
- decide whether EmpowerEd North can safely and appropriately meet a learner's needs;
- plan and deliver education, support, communication and sensory provision;
- support EHCP outcomes, Preparing for Adulthood and progress reporting;
- safeguard learners and respond to welfare concerns;
- manage attendance, absence, incidents, risk assessments, behaviour support, medical needs and first aid;
- communicate with parents/carers, schools, local authorities, health, social care and other professionals;
- manage staff, volunteers, recruitment, safer recruitment checks, training, payroll and contracts;
- manage finance, insurance, complaints, legal obligations and business administration;
- maintain safe and secure systems, devices and records;
- meet legal, safeguarding, contractual, commissioning and regulatory requirements.

4. Our lawful bases

Our lawful bases may include contract, legal obligation, vital interests, legitimate interests, public task where applicable through commissioned education arrangements, and consent for genuinely optional activities. Where we process special category information, such as health, disability, SEND or safeguarding information, we will also rely on an appropriate special category condition. This may include safeguarding of children or individuals at risk, health/social care purposes, employment/social protection, substantial public interest, explicit consent or vital interests, depending on the circumstances.

5. Who we share information with

Where lawful and necessary, we may share information with parents/carers, placing schools, colleges, local authorities, children's social care, adult safeguarding, health professionals, police, LADO, safeguarding partnerships, DBS, courts, legal advisers, insurers, payroll/accounting providers, IT providers, approved digital systems, regulators and other professionals involved in education, safeguarding, welfare, health, commissioning or legal processes.

We will not sell personal information. We will not share information for publicity or marketing without an appropriate lawful basis and, where required, consent.

6. Safeguarding and confidentiality

We respect confidentiality, but safeguarding comes first. If we believe a child, young person or adult at risk may be at risk of harm, we may share information without consent where this is lawful, necessary and proportionate.

7. How long we keep information

We keep information only for as long as needed for education, safeguarding, legal, contractual, employment, finance, complaint, insurance or regulatory purposes. Different records are kept for different periods. Safeguarding, allegations, employment and finance records may need to be kept longer than routine enquiry records. The working retention schedule is included as an appendix and will be finalised before adoption.

8. How we keep information safe

We use appropriate safeguards such as restricted access, secure passwords, multi-factor authentication where available, approved systems, locked paper storage, staff training, secure disposal and breach reporting. We review security when systems, venues, staffing or delivery models change.

9. Your rights

Depending on the circumstances, you may have rights to be informed, access your data, correct inaccurate data, request deletion, restrict processing, object to processing, request portability, and challenge automated decisions. These rights are not absolute and may be limited where information is needed for safeguarding, legal, employment, contractual, education, complaint or regulatory reasons.

To make a request, contact the Data Protection Lead at admin@empowered-north.co.uk. We may need to confirm identity before responding.

10. Complaints

If you are unhappy with how we use personal data, please contact EmpowerEd North first so we can try to resolve the issue. You can also complain to the Information Commissioner's Office (ICO), the UK regulator for data protection.

ICO website: www.ico.org.uk

11. Updates to this notice

We may update this Privacy Notice when our services, systems, venues, legal duties or data protection arrangements change. The current version will be available from EmpowerEd North.

Learner-friendly privacy summary
This section should be adapted with visuals, symbols, AAC support or discussion where this helps a learner understand.

Question	Answer
Who are we?	We are EmpowerEd North. We support young people with learning, communication, independence, wellbeing and preparation for adulthood.
What information do we keep?	We keep information that helps us understand you and keep you safe. This might include your name, people to contact, what helps you learn, what helps you feel safe, your health needs, your communication, your targets and what you do well.
Why do we keep it?	We use it to plan your support, help you learn, keep you safe, talk to the right people and record important things.
Who might see it?	Only people who need to know. This might include EmpowerEd staff, your parent/carer, your school, the local authority, health or social care workers, or safeguarding people if someone is worried about safety.

Can you ask about it?	Yes. You can ask a trusted adult what information we keep about you. You can also say if something is wrong.
Will we keep everything private?	We keep information private where we can. If someone may be unsafe, we may need to tell the people who can help.
Photos and videos	We will only use photos or videos in ways that have been agreed, unless they are needed for safety or safeguarding.

Appendix A: Pre-start data protection completion checklist

Completion item	Status	Evidence / notes
Data Protection Lead named and contact route confirmed	Recorded in the relevant operational record	
ICO registration / data protection fee position checked and recorded	Recorded in the relevant operational record	
Approved Systems Register completed for email, cloud storage, learner records, website forms, devices and communication tools	Recorded in the relevant operational record	
Commissioner / placing school data-sharing and reporting arrangements agreed	Recorded in the relevant operational record	
Data retention schedule approved	Recorded in the relevant operational record	
Privacy Notice published / available to parents, learners and staff	Recorded in the relevant operational record	
Learner-friendly privacy summary prepared where needed	Recorded in the relevant operational record	
Consent forms checked for images/video, off-site activity and optional processing	Recorded in the relevant operational record	
Data breach log and response route ready	Recorded in the relevant operational record	
Subject access request log ready	Recorded in the relevant operational record	
Processor/supplier checks completed for Microsoft, website host, email, storage and any learner record system	Recorded in the relevant operational record	
Secure paper storage and disposal arrangements confirmed	Recorded in the relevant operational record	
Staff induction includes data protection, confidentiality and information security	Recorded in the relevant operational record	
DPIA completed for any high-risk system or processing before use	Recorded in the relevant operational record	

Appendix B: Record of processing activities - working summary

Processing area	Data used	Purpose	Possible lawful basis	Possible recipients	Main record location
Enquiries and referrals	Learner/parent/ carer/referrer contact details, referral	Responding to enquiries; assessing suitability	Contract steps, legitimate interests, consent where optional	Schools, LAs, professionals where needed	Enquiry/referral file

	information, needs summary				
Admissions and placement setup	EHCP, risk information, contact details, medical, safeguarding, support needs	Decide whether needs can be met; plan safe provision	Contract, legal obligation, legitimate interests, public task where applicable	Commissioners, schools, parents/carers, professionals	Learner file
Education and progress records	Targets, progress, attendance, reports, work evidence, images where authorised	Deliver education and report progress	Contract, legal obligation, legitimate interests, public task where applicable	Commissioners, schools, LAs, parents/carers	Learner file
Safeguarding and welfare	Concerns, disclosures, chronologies, referrals, body maps, agency notes	Protect learners and adults at risk	Legal obligation, vital interests, legitimate interests, substantial public interest/safeguarding condition	DSL, social care, police, LADO, commissioners, safeguarding partners	Safeguarding file
Behaviour, risk and incident records	Risk assessments, PBS plans, incident forms, RPI records, debriefs	Keep people safe and improve support	Legal obligation, legitimate interests, contract, safeguarding condition where relevant	Commissioners, parents/carers, professionals, safeguarding partners where needed	Learner/risk file
Staff and recruitment	Applications, references, DBS/check information, contracts, payroll, training, supervision	Recruit and manage staff safely	Contract, legal obligation, legitimate interests, employment/social protection	DBS, payroll, HMRC, pension, referees, LADO where relevant	Staff file / SCR
Complaints and legal claims	Complaint records, correspondence, investigation notes, outcomes	Resolve complaints and protect legal position	Legal obligation, legitimate interests, contract	Insurers, legal advisers, commissioners, regulators where relevant	Complaint file
Website and communications	Contact forms, emails, newsletter/updates if used, technical logs	Respond to contact; manage communication	Legitimate interests, consent where required, contract steps	Website/email provider, IT support	Email/website records

Appendix C: Data sharing decision checklist

- What information is being requested or considered for sharing?
- Who is requesting it and what is their role?
- What is the purpose of sharing?
- Is there a safeguarding, legal, contractual, education, health, welfare or public interest reason?
- What is the lawful basis and special category condition if applicable?
- Is the information accurate, relevant, necessary and proportionate?
- Could sharing increase risk to the learner or another person?
- Does the learner/parent/carer need to be informed, or would this undermine safeguarding/legal action?
- How will the information be shared securely?
- What record of the decision is needed?

Appendix D: Personal data breach record fields

Field	Record
Date/time discovered	
Person reporting	
Description of breach or near miss	
Data subjects affected	
Type of data involved	
Special category / safeguarding data involved?	
Immediate containment action	
Risk assessment outcome	
ICO report required? Rationale	
Affected individuals informed? Rationale	
Safeguarding implications and DSL informed?	
Learning actions	
Date closed and authorised by	

Appendix E: Subject access request log fields

Field	Record
Date request received	
Requester name and contact details	
Person whose data is requested	
Identity/authority checks completed	
Scope of request	
Deadline	
Systems/files searched	

Third-party data considered/redacted	
Safeguarding/legal exemptions considered	
Response sent date and method	
Outcome/notes	

Appendix F: Working data retention schedule

This is a working schedule and must be confirmed before final adoption. Retention may need to be extended where there is safeguarding risk, complaint, allegation, legal claim, insurance matter, commissioner audit, investigation or statutory requirement.

Record type	Working retention period	Responsible lead
General enquiries where learner does not start	3 years after last meaningful contact, unless safeguarding, complaint or legal reason requires longer retention	Data Protection Lead
Referral/admissions records where learner does not start but significant assessment took place	6 years after decision or longer if safeguarding/legal reason applies	Data Protection Lead / DSL
Core learner education file	6 years after learner leaves, or transfer/return to commissioner where agreed, subject to safeguarding/legal requirements	Data Protection Lead
Safeguarding records	Retain and transfer/share in line with safeguarding guidance and commissioner arrangements; do not destroy without DSL and Data Protection Lead review. Minimum until age 25 should be considered where records are held by EmpowerEd North.	DSL / Data Protection Lead
Allegations meeting harm threshold	Until the person reaches normal pension age or 10 years from the allegation, whichever is longer, unless guidance/legal advice requires longer	DSL / Data Protection Lead
Low-level concern records	Duration of employment plus 6 years, unless pattern/escalation/legal advice requires longer	DSL / Data Protection Lead
Behaviour, incident, RPI and risk records	Retain with learner file; cross-reference safeguarding records where relevant	DSL / Data Protection Lead
First aid and accident records	Minimum 3 years from date of entry, or longer for children/young people, safeguarding, RIDDOR, insurance or legal claim reasons	Health and Safety Lead / Data Protection Lead
Medication records	Retain with medical/learner records according to commissioner and	Data Protection Lead

	health/safeguarding requirements; review before disposal	
Staff recruitment records for unsuccessful candidates	6 months after recruitment decision, unless dispute/legal reason requires longer	Data Protection Lead
Staff employment file	6 years after employment ends, except safeguarding/allegation records which may require longer	Data Protection Lead
Single Central Record	Keep current while active; archive historic entries securely when no longer needed, subject to safer recruitment audit needs	Data Protection Lead
Payroll, tax and finance records	6 years from end of financial year or as required by HMRC/accounting rules	Finance Lead
Complaints records	Minimum 6 years after closure, or longer where safeguarding/legal/insurance issues apply	Data Protection Lead
Visitor logs	Usually 1 year, unless linked to safeguarding, incident, complaint or investigation	Data Protection Lead
Publicity consent records	For as long as image/video is in use plus a reasonable audit period after withdrawal/removal	Data Protection Lead
Website contact form data	As long as needed to respond and manage enquiry, then delete or move to enquiry/referral record if needed	Data Protection Lead
Data breach records	6 years after closure or longer if serious, reportable or linked to complaint/legal claim	Data Protection Lead
Policies and adoption records	Keep current version plus archive of previous versions for governance/audit purposes	Directors / Data Protection Lead