

Sendix Data Processing Agreement, version 1.2 (15 October 2026)

UK GDPR Article 28 agreement between a school, trust or council (the Controller) and Sendix AI Ltd (the Processor). Version 1.2, text of 15 October 2026. Covers EHCPs in England, and Child's Plans and IEPs in Scotland. Schools sign it in the Sendix app and Sendix countersigns. This copy is for review; items in **[SCHOOL]** are completed when you sign.

Between

1. **[SCHOOL]** [school / trust / local authority / Scottish education authority, independent or grant-aided school name], [address], ICO registration [number] (the **Controller**); and
2. **Sendix AI Ltd**, a company registered in Scotland (SC883770), registered office 3F1 Third Floor, 3 Hill Street, New Town, Edinburgh, EH2 3JP, ICO registration ZC264381 (the **Processor**).

This agreement forms part of the agreement under which the Controller uses the Sendix service (the **Main Agreement**). If they conflict on data protection, this agreement prevails. If the Controller is an education authority (a council) and its own contract terms with the Processor conflict with this agreement on data protection, the term that is more protective of data subjects applies.

1. Definitions

Terms such as *personal data*, *special category data*, *processing*, *controller*, *processor*, *data subject* and *personal data breach* have the meanings in the UK GDPR and the Data Protection Act 2018 (**Data Protection Law**).

Service means the Sendix plan review platform, including any optional features the Controller switches on. It covers Education, Health and Care Plans (**EHCPs**) in England and, in Scotland, Child's Plans and Individualised Educational Programmes (**IEPs**), including the **guided IEP review**: checks on each short-term target, questions for staff, suggested wording with a version for the learner, staff decisions, termly review records and a Word export of the meeting summary. **Customer Data** means personal data processed by the Processor for the Controller through the Service.

2. Roles and instructions (Art. 28(3)(a))

2.1 The Controller is the controller and the Processor is a processor of Customer Data.

2.2 The Processor processes Customer Data only on the Controller's documented instructions. Those instructions are: this agreement, Schedule 1, the Controller's configuration and use of the Service, and any further written instructions agreed between the parties. Processing required by law is excepted; in that case the Processor tells the Controller first unless the law forbids it.

2.3 The Processor will tell the Controller promptly if, in its opinion, an instruction infringes Data Protection Law (Art. 28(3)(h)).

2.4 **No secondary use.** The Processor will not use Customer Data for any purpose other than providing the Service to the Controller. In particular it will not use Customer Data, or data derived from it, to train or improve AI models, for benchmarking or analytics across customers, for marketing, or sell or share it. Any such use would need a separate written agreement and a new DPIA.

2.5 **Controller's entitlement.** The Controller confirms it is entitled to process each plan it uploads for the purposes in Schedule 1, including under any information-sharing agreement or terms set by the lead agency.

2.6 **Child's Plans.** Where a Child's Plan is led by another agency (for example a council or health board), the Controller is the controller of its own processing of its copy of the plan, and the lead agency remains the controller of the master plan. This agreement covers only the Controller's copy.

3. Confidentiality (Art. 28(3)(b))

3.1 The Processor ensures that everyone it authorises to process Customer Data is bound by confidentiality and processes it only as needed for the Service.

3.2 Sendix staff do not access Customer Data in the ordinary course. The platform administrator role cannot read plan content, file names, pupil identifiers, follow-through notes or IEP review records through the Service, with no exceptions, including when helping with a data subject request under clause 6. Administrative access to the underlying infrastructure, which could reach the database, is limited to two Sendix staff, protected by multi-factor authentication, and to Sendix's automated deployment pipeline. It is used only for support or incidents the Controller has asked about, legal obligations, or keeping the Service secure, and never to read plan content. Changes to the infrastructure and runs of database jobs are logged; individual database queries are not.

4. Security (Art. 28(3)(c), Art. 32)

The Processor maintains the technical and organisational measures in Schedule 2. It may improve them, but will not reduce the overall level of protection.

5. Sub-processors (Art. 28(2), (4))

5.1 The Controller gives general written authorisation for the sub-processors listed in Schedule 3.

5.2 The Processor will give at least **30 days'** written notice (email to the Controller's contact) before adding or replacing a sub-processor. The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Controller may end the affected part of the Service without penalty.

5.3 The Processor imposes data protection obligations on each sub-processor that are no less protective than this agreement, and remains liable to the Controller for its sub-processors.

6. Data subject rights (Art. 28(3)(e))

6.1 The Processor will help the Controller respond to requests from data subjects (access, rectification, erasure, restriction, portability, objection), taking into account the nature of the processing.

6.2 If the Processor receives a request directly, it will pass it to the Controller within **5 working days** and will not respond itself unless instructed. Requests may come from pupils themselves (in Scotland, a pupil aged 12 or over is presumed able to exercise their own rights). The Processor forwards every request to the Controller and does not assess capacity.

6.3 The Controller's authorised staff can download a data export of each plan themselves through the Service, so access and portability requests are answered by the Controller without the Processor seeing the content.

6.4 On the Controller's written request, the Processor will erase or restrict the relevant Customer Data within **10 working days**, or sooner where the Controller's statutory deadline requires it. It will do the same for any other action the Controller cannot take itself. The Processor acts on the Controller's reference for the pupil or plan, without viewing the content.

6.5 If no remaining member of the Controller's staff has access to a plan, the Processor may, on the Controller's written request, move it to another member of the Controller's staff. Two limits apply:

- **Who can receive plans:** only someone the Controller itself invited to the Service.
- **Notice:** the Processor emails the Controller's billing administrators and SEND leads, and its trust's, each time it does so.

7. Breaches, DPIAs and the ICO (Art. 28(3)(f))

7.1 The Processor will notify the Controller **without undue delay, and in any event within 24 hours**, of becoming aware of a personal data breach affecting Customer Data. Information may be given in phases. The notice will include, so far as known: what happened, the categories and approximate number of data subjects and records, likely consequences, and the measures taken or proposed.

7.2 The Processor will help the Controller with its breach notifications, DPIAs (including by providing and maintaining the Processor's DPIA sections) and any prior consultation with the ICO.

8. End of the Service (Art. 28(3)(g))

8.1 When the Main Agreement ends, the Processor will, at the Controller's choice, return Customer Data in a commonly used format and/or delete it, within **30 days**, and confirm deletion in writing, unless the law requires it to keep the data.

8.2 Copies in backups are overwritten in the ordinary backup cycle, within **35 days**, and are not restored except for disaster recovery.

9. Audits and information (Art. 28(3)(h))

9.1 The Processor will make available the information needed to demonstrate compliance with this agreement. This includes its security pack, Cyber Essentials certificate (once awarded), DPIA sections, sub-processor list, and answers to reasonable written questionnaires.

9.2 If that information is not enough, the Controller (or an auditor bound by confidentiality) may audit on 30 days' notice, no more than once a year unless following a breach or a regulator's request, at the Controller's cost.

10. International transfers

The Processor will not transfer Customer Data outside the United Kingdom without the Controller's prior written consent and appropriate safeguards under Data Protection Law. All sub-processors in Schedule 3 process Customer Data in the UK. The public website sendix.ai is hosted outside the UK (Azure West Europe) and does not receive or process Customer Data. Its enquiry form sends staff contact details straight to the Service in the UK.

11. Liability

Liability under this agreement is subject to the limits in the Main Agreement, except that those limits do not apply to a breach of clause 2.4, 3 or 4 caused by the Processor's negligence.

12. Term, law and jurisdiction

12.1 This agreement lasts as long as the Processor processes Customer Data.

12.2 This agreement is governed by the law of the Controller's home jurisdiction, and the courts of that jurisdiction have exclusive jurisdiction: *England and Wales* for Controllers in England or Wales, and *Scotland* for Controllers in Scotland.

13. Scottish public authorities

13.1 **Freedom of information.** If the Controller is a Scottish public authority under the Freedom of Information (Scotland) Act 2002 (**FOISA**), it may receive requests for information about this agreement or the Service. Before disclosing information that the Processor has identified as commercially sensitive, the Controller will consult the Processor. The decision on disclosure remains the Controller's.

13.2 **Records management.** If the Controller is an authority with a records management plan under the Public Records (Scotland) Act 2011, and that plan extends to records created or held by contractors, the Processor will

cooperate with the Controller to support it, including by providing information about how the Service creates, keeps and deletes records (Schedule 1 and (Sendix's retention schedule, available on request) and by deleting or returning records as clause 8 provides.

Schedule 1: Details of processing

Schedule 1 has two parts. **Part A** applies to Controllers in England and **Part B** to Controllers in Scotland. A Controller reads only its own part. Rows are not shared between the parts.

Part A: England (EHCPs)

Subject matter	Review of Education, Health and Care Plans against statutory requirements, and suggested wording for professional review. Where the Controller switches on follow-through: a checklist of the plan's Section F provision, a termly record of whether that provision was delivered, and an annual review report built from those records.
Duration	The term of the Main Agreement, plus the return/deletion period in clause 8
Nature and purpose	Upload; removal of the pupil's name and identifiers; storage; AI-assisted analysis; staff review (accept, edit or reject); export of the review report and suggested wording. Where follow-through is switched on: staff record each term whether each Section F provision was delivered; the Service keeps an attributed history of changes and produces an annual review report for the Controller to download. Follow-through uses no AI processing.
Personal data	Content of EHCPs, including health, disability, social care and SEN information (special category data), with the pupil's name, NHS number, UPN, postcodes and dates removed. Sections C, D, G and H (health and social care needs and provision) are not stored: only whether each is present and its approximate length. Names of parents, carers and other family are replaced with their relationship, and professionals' names with their role, on a best-effort basis; names of other people in a plan may remain. Staff users' names and work email addresses. Where follow-through is switched on: • for each provision and term: delivery status, a reason chosen from a fixed list, the type of provider, a next action (up to 200 characters) and a staff note (up to 280 characters); • who made each entry or correction, and when; • the plan's review date and closure details. Staff are told to keep names, contact details and dates of birth out of notes. A filter removes the common forms of these, but on a best-effort basis, so a note may still contain personal data, including special category data . Delivery dates in notes are kept.
Data subjects	Children and young people with EHCPs; parents, carers and other family members named in plans; professionals named in plans; Controller staff using the Service
Retention	[SCHOOL] retention period for review records, configured in the Service and applied by the daily retention job (defaults in (Sendix's retention schedule, available on request). Deletion is also carried out on written instruction. Follow-through records: • Open follow-through: a plan with open follow-through is not deleted for age. • Closure: follow-through is closed by the Controller's staff (when the plan is replaced or the child leaves), and only after the latest annual review report has been downloaded. Termly records are deleted 30 days after closure. A closure record is kept so the plan cannot reopen. • Replaced plans: the old plan's records are kept until the replacing plan's review date or its closure, and for 15 months (followed by the 30-day period) if neither is recorded. That 15-month minimum also applies if the replacing plan is erased. • Inactive plans: open follow-through with no activity for 18 months is closed automatically and its termly records are deleted 30 days later, so nothing is kept indefinitely. From 15 months the Service warns the Controller and shows the closing date. Staff can keep a plan open by confirming the child is still on roll; that confirmation is recorded and attributed. • Follow-through records are always deleted with their plan.

Part B: Scotland (Child's Plans and IEPs)

Subject matter	• Child's Plans: review of whether each action in a GIRFEC Child's Plan addresses the wellbeing need it is for, and suggested wording for professional review. • IEPs (guided IEP review): review of each short-term target against Education Scotland practice guidance on measurable targets; questions for staff; suggested wording with a version for the learner; staff decisions; termly review records; and a meeting summary for staff to download. IEPs are not statutory, so the review rests on practice guidance, not legal duties.
Controller of a Child's Plan	The Controller is the controller of its own processing of its copy of a Child's Plan. Where another agency leads the plan, that agency remains the controller of the master plan (clause 2.6). The Controller confirms its entitlement under clause 2.5.

Conditions	• DPA version: the Service accepts Child's Plans and IEPs only from an organisation whose countersigned DPA is v1.2 or later. Earlier versions cover EHCPs only, and the Service refuses Scottish plans under them. • Scottish framework: the guided IEP review is available only to organisations set up under the Scottish framework. • Pause: the Processor can pause new data for one organisation (no new uploads or analyses; existing plans stay readable and exportable) without ending this agreement, for example while a go-live condition is not met.
Duration	The term of the Main Agreement, plus the return/deletion period in clause 8
Nature and purpose	Both plan types: upload (or, for IEPs, pasting a learner profile and targets); removal of the pupil's name and identifiers; storage; staff review (accept, edit or reject). Follow-through is not available for Scottish plans. Child's Plans: extraction of six labelled fields; AI-assisted check of whether each action addresses the wellbeing need, with suggested wording for staff to accept, edit or reject. There is no export of a corrected Child's Plan. IEPs: extraction of the learner profile, targets and views; rule-based checks of each short-term target and of the plan (no AI); questions for staff; on a member of staff's request, AI-suggested wording for one target and a version for the learner; staff decisions (use as a draft, edit or reject); termly review of each target (met, partly met or not met, and why); and a Word meeting summary built only from staff decisions, for the Controller to download.
Personal data	Child's Plans: the text of six labelled fields: wellbeing need, action, responsible service, outcome, review date and lead professional. These fields can contain health, wellbeing, family and social work information (special category data). Each field ends at the next heading of any kind. Text before the first field heading, and text under any other heading, is not kept; this includes headings such as health, medical, social work, chronology, family history, child protection, risk, police and children's hearing. The child's name, NHS or CHI numbers, Scottish Candidate Numbers, UPNs, postcodes and dates are removed, except the plan's labelled review date. Other people's names are replaced with their relationship or role (including Scottish roles such as Principal Teacher, Pupil Support Assistant and Named Person), on a best-effort basis; names of other people may remain. IEPs: the learner profile, strengths and needs; each short-term target with its row (who supports, how, success criteria, by when, review date and the learner's own version); long-term targets; the plan's review date; the child's views and the parents' or carers' views; the accessible version; and the stage (P1 to P7 or S1 to S6 only, never a class name). This can include special category data. Text under a heading for health, medical information, medication, social work or social care is not stored: only the fact that such a section was present is kept. Dates are kept, because target and review dates are the content of an IEP; only a date labelled as a date of birth is removed. The child's name, other people's names (best-effort, as above), NHS or CHI numbers, Scottish Candidate Numbers, UPNs, postcodes, email addresses and UK phone numbers are removed. IEP review records: suggested wording; each decision and the wording chosen; a reason for keeping a target as written (optional); each termly outcome and why; and which member of staff made each entry, and when. Text typed by staff goes through the same name and identifier removal before storage. Staff users' names and work email addresses.
Data subjects	Children and young people with Child's Plans or IEPs; parents, carers and other family members named in plans, or whose views a plan records; professionals named in plans, including from health, social work and other agencies; Controller staff using the Service
Retention	[SCHOOL] retention period for review records, configured in the Service and applied by the daily retention job (default 90 days from upload (Sendix's retention schedule, available on request). Deletion is also carried out on written instruction. • Child's Plans follow that ordinary period. • IEPs with no review activity follow that ordinary period. • IEPs with review activity are not deleted for age until 18 months (548 days) after their last review activity, plus a 30-day grace period. After that, the ordinary period counted from upload applies, so the IEP is normally deleted at the next daily run. Review activity is asking for suggested wording, recording or reopening a decision, or recording a termly review; uploading alone is not activity. • Confirm still in use: after 15 months without review activity, the Service flags the IEP for staff to confirm it is still in use. Recording a termly review restarts the period. • The hold only adds time. A longer period set by the Controller still applies, and the hold does not affect erasure on instruction or deletion at the end of the Service. • IEP review records (suggestions, decisions and termly reviews) are kept with their IEP and deleted with it.

Schedule 2: Technical and organisational measures

These are measures in place on the date of approval. Planned measures are listed separately and are **not** commitments that have already been met.

Hosting and location

- Application, database, secrets and logs in Microsoft Azure **UK South**. AI inference in AWS **London** (eu-west-2), in-region only.
- Data encrypted in transit (TLS) and at rest (Azure and AWS platform encryption). Secrets held in Azure Key Vault.

Minimisation

- The pupil's name, NHS numbers, UPNs, postcodes and dates are removed before storage or AI processing. The upload is refused if the name cannot be reliably removed. For IEPs, dates are kept except a date labelled as a date of birth, and email addresses and UK phone numbers are also removed.
- For Scottish plans, Scottish Candidate Numbers (9 digits) and CHI numbers are also removed: when labelled, in any spacing; unlabelled, when written as a standalone 9-digit number (SCN) or a 10-digit number (CHI, caught by the NHS number pattern).
- For Child's Plans, only the six labelled fields are stored. Each field ends at the next heading of any kind, and text under health, social work, chronology, family, child protection and similar headings is discarded.
- For IEPs, only the parts the review uses are stored (Schedule 1). Text under a health, medical, medication, social work or social care heading is discarded, and only the fact that it was present is kept.
- Sections C, D, G and H of an EHCP are parsed only to find section boundaries. Their text is discarded, and only whether each section is present and its approximate length are kept.
- Names of people other than the pupil are replaced before storage and before any AI processing: family members with their relationship, professionals with their role (including Scottish school roles). This is best-effort, and some names may remain.
- The original file is not stored by the server.
- The AI model receives extracts, not whole plans:
 - **Child's Plans:** the wellbeing need and the action;
 - **IEPs:** nothing on upload. Only when a member of staff asks for suggested wording for one target does the model receive the learner profile, strengths, needs, the child's and parents' views, and that target and its row. Names are removed again before the call.
- Follow-through notes are short (280 characters), and the field asks for objective facts. Before storage, a filter removes email addresses, UK phone numbers, NHS numbers, UPNs, postcodes and labelled dates of birth. It is best-effort, not a guarantee. The field also warns staff when a note appears to name the child or a titled person.

Access control

- Plans belong to the school.
 - **Who can see them:** only the school's SENCOs and SEND leads, and its trust's SEND lead.
 - **Condition:** only while the contracting organisation (the trust, or the school if it has no trust) has a countersigned agreement and has not been offboarded.
 - **Plans with no school** stay with the member of staff who uploaded them.
- **Leavers:** someone the school removes loses access, including to plans they uploaded.
- **Other roles:** IT leads, billing administrators, other schools and Sendix administrators cannot see plan content through the Service.
- Drafts stay with their author.
- The guided IEP review is available only to schools set up under the Scottish framework. IEP review records follow the plan's access rule.
- Child's Plans and IEPs are accepted only from an organisation whose countersigned DPA is v1.2 or later. The Service refuses them under an earlier version.
- Automated tests in the build pipeline try every protected record route as a user from another school, trust or role. A new route cannot be released without such a test.
- Follow-through records follow the plan's access rule.
 - A save that would overwrite a colleague's change to the same provision is refused.
 - Every change records who made it and when.
 - Unsaved notes in the browser are tied to the signed-in user, and are cleared on sign-out or when the session ends.
- Passwords: at least 12 characters, checked against a deny-list.

- Lockout after 5 failed attempts. Rate limiting.
- Sessions expire after 30 minutes idle, and are revoked on password reset, sign-out or role change.
- **Multi-factor authentication is mandatory for Sendix administrators and for Controller SENCO and SEND lead accounts**, and available to other Controller staff.

AI controls

- Only approved models in approved UK regions can be called (fail-closed policy). The provider does not retain inputs or use them for training.
- Every suggestion requires a staff decision. Only accepted changes are exported.
- IEP checks and questions are rule-based and use no AI. Suggested IEP wording is shown only if every number, role, date and content word in it can be traced to the plan. Anything the plan does not say is shown as a gap in square brackets, for staff to fill in, or no suggestion is offered.

Application security

- Strict security headers and an enforced content security policy.
- Dependencies, container images and the code history are scanned for vulnerabilities and secrets on every change and weekly. High and critical fixes are applied within 14 days.
- Personal data is excluded from application logs.
- A separate staging database. Build systems never receive production database credentials.

Organisation

- Confidentiality obligations for all staff.
- Audit log of security-relevant actions (role changes, lockouts, MFA events, data exports and plan hand-overs).
- The Controller's billing administrators and SEND leads are emailed whenever Sendix hands plans to another member of their staff.
- Documented admin-access and break-glass procedure.
- A per-organisation pause: Sendix can stop new uploads and analyses for one organisation (and, for a trust, its schools) without ending this agreement. Existing plans stay readable and exportable. Pausing needs a recorded reason and is audit-logged.
- Incident response with notification within 24 hours (clause 7).

Retention and data subject rights

- A daily retention job deletes records once their retention period ends, with periods set per organisation and a dry-run preview.
- The Controller's own staff can download a data export for each plan.
- Erasure and restriction of one pupil's records, staff account deletion, and organisation offboarding with a deletion certificate.
- A documented runbook for data subject requests, using the deadlines in clause 6.

In progress: Cyber Essentials. Sendix applied and paid on 9 October 2026, and the certificate is pending.

Planned (not yet in place):

- **Independent penetration test.** A focused test of cross-school access and the release checks, commissioned when the first paid engagement is signed and completed before the first school's real pupil data is processed. Sendix shares the summary with the Controller before its real plans are uploaded.
- Improving the accuracy of other-name redaction (currently 82–88% on test sets).

Schedule 3: Authorised sub-processors

Sub-processor	Service	Location of processing
---------------	---------	------------------------

Microsoft Ireland Operations Ltd (Microsoft Azure)	Hosting, database, key management, logging	United Kingdom (UK South)
Amazon Web Services EMEA SARL (AWS Bedrock)	AI model inference on extracts of plans	United Kingdom (London, eu-west-2)
Amazon Web Services EMEA SARL (AWS SES)	Transactional email to staff (no child data)	United Kingdom (London, eu-west-2)

Signatures

This agreement may be signed electronically, including by click-signature in the Service. The signatory for the Controller confirms they are authorised to sign on behalf of the Controller.

	Controller	Processor
Name	[SCHOOL]	[Founder name]
Role	[SCHOOL]	Director, Sendix AI Ltd
Authority	The signatory confirms they are authorised to sign on behalf of the Controller	
Signature		
Date		
DPA version	1.2	1.2 (recorded on countersignature)

Who signs for the Controller. The organisation that controls the pupils' data, through someone it has authorised: the academy trust for an academy or free school; the governing body for a maintained school; the proprietor for an independent school; the board of managers for a grant-aided school; and the council (as education authority) for a Scottish council school. In the app the signatory types their full name and role and confirms they are authorised to sign on behalf of the organisation; all three are recorded with the date and version, and the app shows the same guidance on the signing step.