Data Processing Agreement, version 1.4

Sendix · Approved 6 November 2026 · goes with DPIA v0.7 · November 2026

Version 1.4 · in force for every new signature

UK GDPR Article 28 agreement between a school, trust or Scottish council (the Controller) and Sendix AI Ltd (the Processor). Version 1.4, approved 6 November 2026. Goes with DPIA v0.7. Covers EHCPs in England, with optional review preparation, and Child's Plans and IEPs in Scotland, with optional delivery tracking, including for Coordinated Support Plans. 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]** [the controller: the academy trust; the governing body of [school]; the proprietor of [school or provision] (legal name, and company or charity number); the local authority for a pupil referral unit; or the Scottish education authority, or independent or grant-aided school], [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, Coordinated Support Plans (CSPs) 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. In England it also covers **review preparation**: where the Controller switches it on, help for its staff in preparing the annual review of an EHCP (Schedule 1, Part A). **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 (including LA case references, UPNs, pupil display names and name hashes), follow-through notes, delivery records, IEP review records or review preparation 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 held by one Sendix founder, protected by multi-factor authentication, and by 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.

Legal holds. The Controller's staff can place a legal hold on a plan (delivery routes) where its records may be

needed for a legal claim. If an erasure request covers a plan under an active legal hold:

- **(a) Only the held records are paused.** The Processor erases every record the request covers that is not under a hold, within the period above, and pauses only the held records.
- **(b) Notice.** Within **2 working days** of receiving the request, the Processor tells the Controller which records are held and paused, and when and by which role each hold was placed.
- **(c) The decision is the Controller's.** Whether an exemption from erasure applies (for example UK GDPR Article 17(3)(e), legal claims) is for the Controller to decide. The Processor does not decide it, and its messages to the Controller and the requester state only that the records are held at the Controller's instruction.
- **(d) Confirmation.** The Processor erases the held records within **5 working days** of written confirmation, from the Controller's DPO or the contact the Controller has named for data protection, that the erasure should go ahead. Before acting, the Processor verifies the confirmation by calling the Controller on a number it already holds, not one given in the confirmation. It records who confirmed, when, the Controller's reference and the call-back on the hold.
- **(e) Release.** The Controller's staff can release a hold at any time, with a reason. Releasing a hold does not erase anything by itself.

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.

8.3 **Plans under a legal hold.** If any plan is under a legal hold when the Main Agreement ends, the following applies. Days are calendar days counted from the day the Main Agreement ends.

- **(a) Full record.** The Processor tells the Controller which plans are held and offers the full record of each, for the Controller's staff to download through the Service.
- **(b) Reminders.** If a held plan's full record has not been downloaded, the Processor reminds the Controller's contacts on **day 14** and **day 21**.
- **(c) Deletion.** The Processor deletes the held plans with the rest of the Customer Data by **day 30**, as clause 8.1 provides, whether or not their full records have been downloaded.
- **(d) One extension.** Before day 30, the Controller may ask in writing for one extension of up to **60 days** for the held plans only. The Service stays available to the Controller's staff for those plans alone, to download their records. They are deleted at the end of the extension.
- **(e) The Controller's instruction prevails.** A written instruction from the Controller about held plans (to

return, delete or keep them for the extension) prevails over this clause and over the Service's own checks. The Processor does not keep Customer Data for the Controller's legal claims beyond the periods in this clause.

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

9.1 The Processor will make available the information needed to show that it meets its obligations under 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 labelled full dates of birth, and the other date forms listed in Schedule 2, removed from the stored plan text (where delivery routes are switched on, the LA case reference and UPN are stored separately: see below; where pupil display names are switched on, the name is stored separately: see below). **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.
Delivery routes: subject matter	Where the Controller switches on delivery routes (optional): recording who delivers and funds each Section F provision and whether it was delivered each term; asks to the local authority and their follow-up; reminders of statutory and locally recorded dates; and documents built from those records for the Controller's staff to download. Delivery routes use no AI processing.
Delivery routes: nature and purpose	• **Identifiers:** staff type the LA case reference and, optionally, the UPN on the plan, import them from the Controller's own tracker, or keep one found in an uploaded plan (an offer that is unticked by default). Each is attributed to the member of staff and audit-logged by field name only. • **Imports:** a tracker or provision-map file (CSV or .xlsx) is read **in memory only** to match its rows to the Controller's plans, and is not kept. Rows are matched by UPN or LA case reference. A tracker row that matches no plan is kept as a pending row for up to 30 days and may be matched to a later upload by a keyed name hash. A match is a suggestion that applies only when a SENCO confirms it. • **Delivery records:** staff (or, for assigned plans, a SEND assistant) record each term whether each provision was delivered, with the period and the source; "not happening" records; recovery actions; delivery groups; standing routes; provision hours. • **Asks and reminders:** asks to the LA, their history and chases; reminders computed from the plan's dates and the events staff enter; an optional calendar feed for each member of staff. • **Legal holds:** the Controller's staff can place a hold on a plan, which stops deletion for age (clause 6.4 and 8.3). • **Documents:** routine exports, the full record of a plan, and the outstanding asks report, downloaded by the Controller's staff. Where the Controller requires it, a routine export is approved by a named role first.

Delivery routes: personal data	• **Identifiers:** the LA case reference; the UPN (optional); the child's year group; whether the plan is a draft for consultation. These structured records are stored apart from the plan text and are never supplied to the AI model. They are identifying, not pseudonymous. An LA case reference written in the text of a plan is not generally removed (Schedule 2). • **Name hashes (temporary):** for a tracker row that matches no plan, a keyed hash (HMAC-SHA256) of the child's normalised name, and of the name with the date of birth where the tracker has a date of birth column, kept with the row's LA case reference, UPN, year group and review dates for **up to 30 days**. • **Name hash (persistent, opt-in):** only where the Controller opts in for a school, one keyed hash of the child's name per plan, kept until the plan is deleted, used only to match provision-map rows to that plan. • Name hashes are **pseudonymised personal data**: someone holding the key could test a guessed name. They are never shown, exported or logged. The key is held as described in Schedule 2. • **Not stored:** names, dates of birth and every other column in an imported file are processed in memory only, and never stored or logged. A pupil name typed on screen (to redact a plan or to put initials in a chase) is used in memory only, unless the Controller has switched on pupil display names and a member of staff confirms it as the display name. • **Delivery records:** for each provision and term, the status, period, source and a staff note (scrubbed as follow-through notes are, best-effort); "not happening" records with a reason code; recovery actions (fixed type, owner, due date, linked ask); delivery and funding roles; provision hours; provision-map rows (quantities, the adult's role code and the file's fingerprint). • **Asks:** a one-line summary, the recipient, dates, a decline reason and the reasons for next steps (all scrubbed, best-effort, so a name the filter does not recognise may remain), with an attributed history and chases. • **Reminders:** the events staff enter (review meeting, amendment notice, draft received, assessment request received, whether a phase transfer applies) and what staff record against a reminder (the LA's date, done or dismissed with a one-line reason, the ask made). • **Groups:** a group name (scrubbed), the adult's role, optional sessions and minutes, a count of other pupils on SEN support (never who), and which plans and provisions belong to it. • **Legal holds:** who placed and released each hold, their role, when, the reason (scrubbed), and any erasure confirmation with its call-back. • **Calendar feeds:** for each member of staff, a fingerprint (SHA-256) of the feed's secret address and how often it is used. Feed events name no child: they show the LA case reference or the Sendix reference. • **Export approvals:** a fingerprint of the approved export, the approving role and the date. • **Staff:** the names of the Controller's SENCOs, SEND leads and SEND assistants where shown as recovery owners; sign-off assignments; the school's termly teaching assistant hours.
Delivery routes: data subjects	Children and young people with EHCPs; family members or other people named in notes, ask summaries or group names despite the filter; Controller staff, including SEND assistants
Delivery routes: retention	Controller-approved defaults, to be confirmed by the Controller (Sendix's retention schedule, available on request): • **Pending tracker rows and their name hashes:** deleted when linked to a plan, or **30 days** after import, by a daily job that runs whatever the retention setting. Expired rows are never matched. • **Identifiers, including any persistent name hash:** deleted with the plan. The persistent hash is also deleted if the Controller withdraws its opt-in for the school. • **Delivery records, provision-map rows, routes, hours, asks, reminders, entered events and export approvals:** deleted with the plan, or with its termly records after follow-through closes. • **Groups, sign-off assignments for a caseload and teaching assistant hours:** until the Controller's staff delete them, and at the end of the Service. • **Calendar feeds:** until the member of staff turns the feed off or regenerates it, their account or membership ends, or the Service ends. • **Legal holds:** a held plan and its records are not deleted for age. Erasure follows clause 6.4 and the end of the Service clause 8.3.
Review preparation: subject matter	Where the Controller switches it on (optional; England EHCPs only): helping staff prepare the annual review of an EHCP. The Service holds the plan's outcomes and the evidence staff add, helps staff weigh that evidence against each outcome, records staff judgements, and produces a write-up for the Controller's staff to download. The Service makes no decision about a child and sends nothing to a local authority, family or professional.
Review preparation: conditions	• **Feature:** behind a separate gate, off by default. It needs follow-through switched on and a plan owned by an organisation. The DPA version required is **v1.4 or later**, held by the contracting organisation. For a trust, every school must qualify. With `ANNUAL_REVIEW_ENABLED` false, non-demo pilot eligibility requires the allow-list, countersigned DPA v1.4 or later and release checks. Setting that global flag true bypasses the annual-review eligibility/version checks. It must remain false for this approval. Analysis is controlled by a separate global flag checked when a run starts; disabling it does not stop queued jobs. This approval does not authorise enabling real-pupil analysis. Before real-pupil analysis is enabled, implement per-organisation authorisation and a worker-side analysis-disable check. • **AI analysis:** behind its own switch, off by default. **It is off for real pupil data at the date of this version.** Analysis stays off until the founder records a release decision after an evaluation labelled by a SENCO. The decision is recorded in the DPIA, and the Processor tells the Controller first. Every other step works without it: staff then find the evidence themselves. • **Demo organisations** hold fictional data only.

Review preparation: nature and purpose	• **Starting a review:** staff start a review of the plan for an academic year, with a meeting date and an internal deadline. • **Outcomes:** staff upload the plan through the existing upload route. Rules, not AI, read the stored Section E text and propose the plan's outcomes. Staff confirm or remove each one, add any that were missed (filtered as staff text, so ordinary dates remain), and link outcomes to Section F provision. Only confirmed outcomes go further. • **Evidence:** staff upload (PDF or Word, up to 10 MB) or paste teacher reports, parent views, child views, assessment summaries and professional reports, and record each source's author role and date. **Staff knowledge:** staff can also type what they know about the child's progress, as a source with a role and date. The original file is not kept. The text goes through the filter in Schedule 2 and is stored in passages of up to 3,000 characters. Staff can delete a document or a passage. Reports are accepted whole, and staff are told to add only what the review needs. • **Parent and child views:** staff must read the filtered text and confirm it before these views can be analysed. • **AI analysis (only where switched on):** a member of staff starts it. In a successful run, for each confirmed outcome, the model reads **each eligible passage, in batches, not extracts**, twice: once to find statements about the child's progress towards that outcome, for and against, and again to look for anything against that was missed. Documents lacking an author role or date are skipped, and a failure can stop processing early. Quotes must be copied exactly. The Service checks each quote against the stored text and drops any that does not match. The proposal stage then receives the outcome, validated evidence items with source metadata, and review window, and suggests a status (working, partly working, not working, not enough evidence yet or achieved) with a reason that cites the source's role and date for each sentence. If a check fails, no suggestion is shown. • **Staff judgement:** staff can dismiss or restore a quote and add exact quotes of their own. For each outcome a member of staff records a status and a reason. A suggestion is never a decision and never overwrites one. Each decision is attributed, with its history. Termly delivery records for linked provision are shown beside the evidence, and a copy is kept with the decision. Structured identifier records, delivery records and meeting records are not supplied to the review model. Review text is filtered for recognised identifier patterns. LA case references and identifiers in unrecognised forms may remain in evidence and may reach the model when analysis is enabled. Staff must exclude unnecessary identifiers. General LA-reference removal is not currently implemented. • **Changes staff record:** staff can type replacement outcomes. Staff can record a recommendation about provision only as an exact quote from a professional report, where the professional's role is confirmed and matches who delivers that provision in the plan. Staff accept or reject it. No model wording is used. • **Meeting record:** attendee roles, notes, and actions with an owner's role and a due date. These are never sent to the model. • **Write-up:** a Word document for the Controller's staff to download, built from confirmed outcomes, staff decisions, quotes staff added, quotes the model found that staff have actively selected (staff must actively select a quote the model found before it reaches the write-up. This is a requirement in force before AI analysis is released.), delivery records, notes, actions, replacement outcomes, accepted recommendations, and submitted parent and child views in full, without the analysis-confirmation check. Suggested statuses are not included. Where the Controller requires it, a named role approves the write-up first. The child's name, typed by staff, is put into the document for that download and is not stored.
Review preparation: excluded proposed designs	AI suggested changes and school-template processing are excluded from current processing instructions. The descriptions below are proposed designs, not implemented controls. Activation requires an updated processing specification and DPIA, applicable privacy information, and the Controller's express documented instruction. Any material departure from this Schedule requires an agreed written variation before processing. • **AI suggested changes:** the model would suggest changes to outcomes and provision from the same evidence, showing the source of each suggestion. Staff would keep, edit or reject each one. Nothing would change without a staff decision, and provision changes would rest on a named professional source. • **School template:** the Controller would upload a blank review template, its own or its local authority's, which would be stored encrypted and held for the organisation. Staff would map its fields, and the write-up would be filled into it for staff to check and download.

Review preparation: personal data	• **Outcomes:** the outcome text from the plan (filtered as plan text) or added by staff (filtered as staff text, so ordinary dates remain), its reference, timeframe and area of need, and links to Section F provision. • **Evidence text:** the full filtered text of each report, view and staff knowledge entry. This can include health, medical, therapy, psychological, family and social care information (**special category data**). The rule that Sections C, D, G and H are not stored applies to plan text. It does not apply here: **reports are kept whole**, including any health content, and no text is discarded by heading. • **Dates are kept in review evidence**, because the date of an observation is part of the evidence. Only a labelled date of birth written in a recognised complete-date pattern is removed. A labelled partial date, or a date of birth with no label, stays. • **Source details:** kind of document, author role, professional domain, document date, a random file name, a fingerprint of the filtered text, and who uploaded and confirmed it. • **Analysis records (only where AI analysis is switched on):** each quote (up to 600 characters) with its stance, role and date; the suggested status, reason and warning flags; the recorded model ID and prompt version; run status. • **Staff records:** each decision (status, reason, stage, who, role, when) with its history and delivery copy; quotes staff add; recommendations and the decision on each; replacement outcomes; meeting attendee roles and notes; outcome notes; actions. • **Not stored:** the child's name. Staff type it for each piece of text they save and for each write-up. It is used in memory to remove the name, and held in that browser tab's memory only, unless the Controller has switched on pupil display names. The filter is best-effort for anyone other than the child, so a report or staff knowledge entry may still name family members, professionals or other children.
Review preparation: data subjects	Children and young people with EHCPs; parents and carers whose views are recorded; family members, other children and other people mentioned in reports or staff knowledge despite the filter; teachers and professionals who wrote or are named in reports; Controller staff
Review preparation: retention	Controller-approved defaults, to be confirmed by the Controller (Sendix's retention schedule, available on request): • **Evidence text:** When retention enforcement is enabled, the daily job deletes evidence passages 30 days after finalisation or cancellation. For an open review, deletion falls 180 days after the latest review creation/update or plan-level annual-review activity. An active legal hold suspends this deletion. Document metadata and saved quotes, including dismissed quotes, remain with the plan unless separately deleted or replaced. Passage deletion removes the source passages from later exports, including the full parent and child views; it does not delete saved quotes. • **All other review records:** deleted with the plan. • **Legal holds:** a held plan's evidence text is not deleted for age (clause 6.4 and 8.3). • **School templates (proposed design, excluded above):** until the Controller's staff delete them, and at the end of the Service.
Pupil display name: subject matter	Optional, off by default, switched on per school by the Controller, and in effect once built (**not built at the date of this version**): showing staff the name of the child each plan and review relates to, so that they can manage their caseload and open the right review. Uses no AI processing.
Pupil display name: conditions	A separate feature gate, off by default, and a per-school switch set by the Controller. Requires a countersigned DPA v1.4 or later. England only. The shortest usable name. No SEND assistant access initially. Trust lists show references only. Demo organisations hold fictional names only.
Pupil display name: nature and purpose	Staff confirm the name suggested from the plan, or type it. The Service stores it apart from the plan text, shows it to staff who can access the plan, prints it in review documents staff choose to generate, and uses it to remove the child's name from later text.
Pupil display name: personal data	One display name for each plan, in the shortest usable form, up to 80 characters. No date of birth, photograph, address or other field. It is identifying and is held with the plan it relates to, so anyone who could read both would know whose plan it is. It is never sent to the AI model.
Pupil display name: data subjects	Children and young people with EHCPs
Pupil display name: retention	Deleted with the plan; on the Controller's instruction; when the Controller switches the feature off for the school (in the next daily run); and at the end of the Service.

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

Optional delivery-record personal data: education-authority case reference, optional pupil number, matching hashes (persistent only on school opt-in), recorded coordinator contact, objective/support/provider text,

dated delivery records, asks, reminders, staff attribution and legal holds. These are identifying data, kept separately from redacted model input. Staff check all wording; no automated decision changes a child's entitlement.

Optional delivery records are covered for Scottish plans by v1.3. Child's Plans, IEPs and Coordinated Support Plans (CSPs) are eligible under the existing delivery-routes flags and a countersigned v1.3 or later. Automated CSP analysis remains separately subject to corpus validation. No agreement has yet been issued under v1.3; this scope is incorporated before issue.

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	**Child's Plans and IEPs:** 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). Optional delivery records cover all three Scottish plan types: objective/action/target routes, additional support and providers, coordinator chase contact, delivery checks and recovery actions, education-authority and provider asks, reminders, imports, groups, legal holds and calendar feeds. The identifier, name-hash opt-in, in-memory matching, access, encryption, retention and deletion safeguards in Part A's delivery-record scope apply equally. The education authority remains responsible. CSP records include the educational objectives, additional support and persons/agencies providing it; review dates under s.10 and appropriate-agency help under s.23. Child's Plan and IEP review dates are locally agreed, not statutory. **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, labelled full dates of birth and other 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 labelled date of birth written in a recognised complete-date pattern 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.
- **Review preparation text** has field-level encryption as well (AES-GCM, with each column bound separately), under the key used for stored identifiers: evidence passages, quotes, suggested and decided reasons, decision history, recommendations, replacement outcomes, meeting notes, outcome notes and actions. Outcome text, statuses and document details rely on platform encryption.

Minimisation

- The pupil's name, NHS numbers, UPNs, postcodes and labelled full dates of birth are removed from the plan text before it is stored or sent for AI processing. For EHCP plan text, numeric dates (such as 12/05/2026 or 12.05.26) and dates written as a day, month and year (12 May 2026) are also removed. Other forms, such as "12th May 2026" or "May 2026", can remain. The upload is refused if the name cannot be reliably removed.

- **Stored identifiers.** Where delivery routes are switched on, the LA case reference and the optional UPN are stored apart from the plan text (Schedule 1). The structured records are never supplied to the AI model. UPNs in recognised forms are removed from plan text. General LA-reference removal is not currently implemented, so an LA reference written in plan text can remain and can reach the model. Both stored values are encrypted at field level (AES-GCM) under a key held in Azure Key Vault. For IEPs, dates are kept except a labelled date of birth written in a recognised complete-date pattern, and email addresses and UK phone numbers are also removed.
- **Pupil display names.** Where the Controller switches them on for a school, once built, one display name is stored for each plan, apart from the plan text, with application-level encryption under a key held in Azure Key Vault and used for nothing else. It is confirmed by staff before it is stored. It is never sent to the AI model, and the Service refuses a model call if the name appears in it. It is kept out of logs, filenames, notifications and calendar feeds. Stored plan text is unchanged: the name is replaced by a placeholder before storage, and the placeholder is filled only in a response to authorised staff or a document they generate. This feature is not built: these are requirements for the build.
- **Review evidence.** Before a report, view or staff knowledge entry is stored, the Service:
    - refuses it if a child's name labelled in the document differs from the name staff typed, or if the child's name cannot be removed;
    - replaces the child's name, and recognised aliases and aliases supplied by staff, with a placeholder;
    - removes NHS numbers, UPNs, postcodes, email addresses and UK phone numbers;
    - removes a date only where it is labelled as a date of birth (for example "DOB", "date of birth" or "born on") and written in a recognised complete-date pattern, and keeps every other date. Labelled partial dates, such as a month and year, and a date of birth with no label, stay;
    - replaces other people's names with a relationship or role, on a best-effort basis, and replaces the file name with a random one.

  Staff text saved during a review (decisions, notes, actions, added and replacement outcomes) goes through the same name, identifier and date steps, but with no alias handling.

  Structured identifier records, delivery records and meeting records are not supplied to the review model. Review text is filtered for recognised identifier patterns. LA case references and identifiers in unrecognised forms may remain in evidence and may reach the model when analysis is enabled. Staff must exclude unnecessary identifiers. General LA-reference removal is not currently implemented.
- 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. This section-discard control applies to the plan-ingestion paths described here. It does not apply to annual-review evidence: an EHCP uploaded or pasted through that route retains its filtered C, D, G and H text.
- 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. Review evidence is the exception:
  - **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.
  - **Review evidence (only where AI analysis is switched on):** in a successful run, each eligible passage, in batches, for each confirmed outcome, not extracts. This is deliberate: evidence against an outcome cannot be found in text the model never reads. Names are removed again before the call. Documents lacking an author role or date are left out, a failure can stop processing early, and analysis does not run on parent or child views until staff have confirmed them.
- 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 written in a recognised complete-date pattern. It is best-effort, so some personal data may remain. The field also warns staff when a note appears to name the child or a titled person. Delivery-routes notes, ask summaries, reasons and group names go through the same filter.
- **Imported files** (trackers and provision maps) are read in memory and not kept. Names, dates of birth and other columns in them are never stored or logged.
- **Name hashes** are keyed (HMAC-SHA256) with a key derived for each school from a secret held in Azure Key Vault, so the same name gives different hashes in different schools. The key itself is never stored in the database. Hashes are never shown, exported or logged. Pending rows that hold them are deleted after 30 days at most.
- Calendar feeds, routine exports and documents for the local authority print no child's name: they use the LA case reference or the Sendix reference. The review write-up that staff download can print the name they type for it, and where pupil display names are switched on, review documents that staff choose to generate may print the name. Routine exports print roles and dates, never staff names, notes or correction history.

Access control

- Plans belong to the school.
  - **Who can see them:** 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.
  - **Uploader:** the member of staff who uploaded a plan also keeps access while they remain a member of that school or its trust, in any role. This does not itself apply the per-plan agreement check; each route's own role and agreement checks still apply.
  - **Plans with no school** stay with the member of staff who uploaded them.
  - **Curated demo reports** are fictional, and are readable by any signed-in user, subject to each route's own checks.
- **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.

- **SEND assistants** (delivery routes): an HLTA or SEND administrator invited by a SENCO or SEND lead to one school. They see only the plans a SENCO has assigned to them for termly sign-off, and for those plans only the LA case reference (or Sendix reference), the Section F provision and its routes, and this term's delivery records, recovery actions and "not happening" records. They cannot see other sections of the plan, other plans, asks, reminders, exports, imports, legal holds, settings or users; every other route refuses the role. Multi-factor authentication is required. Access ends on the next request when the assignment ends, the role is removed or the school is offboarded.
- **Review preparation records** follow the plan's access rule: the school's SENCOs and SEND leads, and its trust's SEND lead. SEND assistants cannot see them. A save that would overwrite a colleague's decision is refused. Starting and finalising a review, saving a decision and downloading a write-up are audit-logged, without the content.
- **Pupil display names** follow the plan's access rule. SEND assistants have no access initially, and trust lists show references only. Other roles and Sendix administrators cannot see them through the Service.
- 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, SEND lead and SEND assistant 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.
- For plan wording changes, every suggestion requires a staff decision and only accepted changes are exported. In review preparation, submitted parent and child views export without the analysis-confirmation check.
- 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.
- **Review preparation.** AI analysis is off for real pupil data (Schedule 1). Analysis stays off until the founder records a release decision after an evaluation labelled by a SENCO. Where it is on:
  - the model is told to treat passages as data, not instructions, and to use only those passages;
  - every stored quote is an exact match to the filtered text;
  - a suggestion of "achieved" or "working" whose citations omit an extracted contrary or mixed item is not shown, and "achieved" with any such item is changed to "partly working" with a warning. This does not catch evidence the model never found;
  - a suggestion that uses barred language or fails a citation check is not shown;
  - evidence from one source only is flagged, and where every quote falls outside the review year the status is "not enough evidence yet";
  - a suggested status never reaches the write-up. Staff must record their own status and reason. Staff must actively select a quote the model found before it reaches the write-up. This is a requirement in force before AI analysis is released;
  - the saved model attribution records `BEDROCK_MODEL_ID`. Calls may use `BEDROCK_MODEL_ROUTES`, so the approval record must cover the routed model.

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).
- **Legal holds** are placed and released by the Controller's SENCOs and SEND leads, with a reason, and audit-logged. An erasure that reaches a held plan follows clause 6.4; confirmations are verified by call-back. The Controller's staff review each active hold at least once a term. This is a manual obligation: the Service prompts only at 365 days.
- **Name-hash key:** the Service refuses to hash if `TRACKER_MATCH_SECRET` is not set, with no fallback. The persistent name hash is kept only where the Controller opts in for a school.
- **Offboarding** of held plans follows clause 8.3.
- **Demonstration organisations** show a permanent "Fictional data only" banner and need a statement on upload that the file is fictional. Uploads not made by Sendix's demonstration set-up are deleted within 30 days.
- **Calendar feeds** are a secret address for each member of staff. Only a fingerprint is stored, the address is shown once, and turning it off or regenerating it revokes the old address. The Service tells staff that anyone holding the address can see the references and dates in it. Feeds show the Sendix reference by default and expire after 180 days by default, and the Controller can turn them off for the organisation.

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. Applied for on 9 October 2026 through IASME. The assessment is under way; no certificate has been issued.

Planned (not yet in place):

- **Independent penetration test.** A focused test of cross-school access and the release checks, booked for January 2027, and complete before a fourth organisation is released. Until it is complete, the Processor releases live pupil data to no more than three organisations in total (schools, trusts and alternative provision all count). It releases an organisation only when the Processor holds a current Cyber Essentials certificate, the cross-school isolation tests pass on the version in production, and the Controller's Data Protection Officer has accepted in writing the residual risks R1 (test pending, with its booked date) and R4 (Medium). The Processor shares the test summary with the Controller when it is

complete.

- Improving the accuracy of other-name redaction, which stays best-effort.
- **AI analysis in review preparation:** off for real pupil data. Analysis stays off until the founder records a release decision after an evaluation labelled by a SENCO. Before real-pupil analysis is enabled, implement per-organisation authorisation and a worker-side analysis-disable check. The global bypass is being removed, and a per-organisation analysis switch added, before analysis goes on.
- **Quotes the model found:** staff must actively select a quote the model found before it reaches the write-up. This is a requirement in force before AI analysis is released.
- **Pupil display names:** not built. Every control in Schedule 1 and above is a requirement before the feature can be switched on.

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 and, where AI analysis in review preparation is switched on, on eligible passages of filtered review evidence	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	1.4	1.4 (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 or an independent alternative provision; the local authority for a pupil referral unit; 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.