DPIA Summary for Leaders

Sendix · Based on DPA v1.4 and DPIA v0.7 · November 2026

A short read for heads, trust leaders, governors and DPOs. It summarises Sendix's own data protection impact assessment (DPIA) so you can decide whether to approve Sendix. Your DPO completes your organisation's DPIA, using the template for your type of organisation in this pack.

1. What Sendix is

Sendix helps SENCOs and SEND leads review Education, Health and Care Plans (EHCPs) in England, and IEPs and Child's Plans in Scotland. Sendix **checks** the wording of a plan, shows the basis for each finding, and **suggests** clearer wording from evidence already in the plan. **A professional decides**: a member of your staff accepts, edits or rejects every suggestion. Only the local authority can amend an EHCP. In England, optional **review preparation** helps staff gather evidence for an annual review and record their own judgement. **Sendix's DPIA v0.7 is provisional:** consultation (Step 3) is outstanding, and it does not authorise a new real-pupil processing release.

2. Why a DPIA is needed

- Plans hold **special category data** (health, disability and special educational needs) about **children**.
- Sendix uses **new technology**: an AI model helps write findings and suggestions.
- The processing is **systematic**: every plan is checked the same way.

3. Roles

Party	Role
Your trust, governing body, proprietor or council	**Controller.** Decides why and how plans are reviewed, chooses the lawful basis, sets the retention period, completes its own DPIA and accepts the residual risk
Sendix AI Ltd	**Processor.** Acts only on the controller's written instructions, under the Sendix Data Processing Agreement (DPA) v1.4
Microsoft (Azure) and Amazon Web Services (Bedrock, SES)	**Sub-processors** to Sendix, listed in DPA Schedule 3 (section 10)
Your SENCOs and SEND leads	**Authorised users.** They read every finding and decide on every suggestion
The local authority (England)	Maintains the EHCP. Only it can amend the plan

4. What data is processed

Children's data. The text of the plan: the child's needs, outcomes and provision. Before anything is stored, Sendix:

- removes the pupil's name, UPNs, NHS numbers, postcodes and most written dates (in Scotland, also Scottish Candidate Numbers and CHI numbers), and refuses the upload if the name cannot be removed;
- **discards the health and social care sections of an EHCP (C, D, G and H)**, keeping only whether each was present and its approximate length;
- replaces other people's names with their relationship or role. This is best-effort, so the stored text is treated as personal data throughout.

The original file is not kept by the server. Sendix holds no MIS data and sends no pupil data by email.

Review preparation (England EHCPs, optional). Reports, views and staff knowledge are stored whole,

encrypted at field level, and the section discard does not apply to them. The filter removes the child's name and recognised identifier patterns, and labelled full dates of birth, and keeps other dates. LA case references and identifiers in unrecognised forms may remain. AI analysis is off for real pupil data. Staff are told to add only what the review needs.

Pupil display names are an optional feature, off by default and switched on per school by you, in effect once built. The AI model never receives the name.

Staff data. Names, work email addresses and roles of the staff who use Sendix; who made each decision on a suggestion, and when; and security events such as sign-ins, lockouts and multi-factor authentication (MFA) changes.

5. Lawful basis

The controller decides the lawful basis, not Sendix. For academy trusts, maintained schools and Scottish councils it is usually public task, Article 6(1)(e), with Article 9(2)(g) and Data Protection Act 2018, Schedule 1, paragraph 6, covered by your Appropriate Policy Document. Independent schools usually rely on legitimate interests, Article 6(1)(f), with an assessment. The DPIA templates in this pack set out the options for each type of organisation, for your DPO to confirm.

6. Where data lives

- **Microsoft Azure UK South:** the application, database, backups, secrets and logs.
- **Amazon Bedrock in AWS London (eu-west-2):** the AI model, called in-region only. On plan review it receives extracts, not whole plans. It **keeps no inputs or outputs**.
- **Backups** stay in UK South and are overwritten within 35 days.
- **No personal data is transferred outside the UK.**

7. Key security controls

- **Plans belong to the school.** Only its SENCOs and SEND leads, and its trust's SEND lead, can see plan text, and only while a countersigned DPA is in place. Leavers lose access.
- **Cross-school isolation tests** run on every change. They try each protected route as staff from another school, trust or role; a build that leaks does not ship.
- **MFA is mandatory** for SENCO and SEND lead accounts and for Sendix administrators. Passwords of at least 12 characters, checked against a deny-list; lockout after 5 failed attempts; sessions end after 30 minutes idle.
- **Sendix staff cannot open plan text in the application.** One person, the founder, holds administrative access to the infrastructure, with MFA. That access could reach the database; individual database queries are not logged. The Security Overview explains this in full.
- **Encryption** in transit (TLS) and at rest (Azure platform encryption, Microsoft-managed keys). LA case references, UPNs and review preparation text also have field-level encryption.
- **Scanning and patching.** Dependencies, container images and code are scanned on every change and weekly; high and critical fixes within 14 days.
- **Breach notice within 24 hours** of Sendix becoming aware (DPA clause 7.1).
- **Certification and testing.** Cyber Essentials: applied for on 9 October 2026 through IASME. The assessment is under way; no certificate has been issued. Independent penetration test: not yet done. It is booked for January 2027, and complete before a fourth is released. See the pilot rule in section 11.

8. AI guardrails

- **Human in command.** Every plan wording suggestion is accepted, edited or rejected by a member of staff, and only accepted changes reach an exported plan. Sendix does not determine EHCP entitlement.
- **AI analysis in review preparation is off for real pupil data.** It stays off until Sendix's founder records a

Sendix AI Ltd · SC883770 · registered in Scotland · ICO ZC264381 · privacy@sendix.ai

release decision after an evaluation labelled by a SENCO. Staff must actively select a quote the model found before it reaches the write-up, a requirement in force before release. Your organisation assesses meaningful human involvement (UK GDPR Articles 22A–22D) before analysis is used.

- **No training.** Bedrock does not store prompts or outputs for this model or use them for training. Sendix does not train or fine-tune any model on your data.
- **Grounded suggestions.** Each finding cites its basis. Suggested wording uses only evidence in the plan; where there is none, Sendix says what is missing instead of guessing.
- **Approved models only.** A model is called only if a signed approval record matches its exact UK endpoint, region and model. Anything else is refused.
- **Clear labelling.** The review panel says that suggestions can be wrong, are not legal advice, and that staff remain responsible for the plan.

9. Retention defaults

Category	Default	Notes
Plan review records (stored plan text, findings, decisions)	90 days from upload	You set your own period in Sendix. A daily job deletes records when it ends (running since 3 October 2026)
Evidence reports	365 days	
Review preparation evidence passages	30 days after a review is finalised or cancelled; 180 days after the latest activity on an open review	Where retention enforcement is on. An active legal hold pauses this. Saved quotes stay with the plan
Deleted drafts	30 days	
Staff invitations	90 days	From acceptance, revocation or expiry
Security logs	730 days	Sign-ins, lockouts, role changes, MFA events. No plan content
Application logs	30 days	No plan text or pupil identifiers
Backups	Within 35 days	Deleted data leaves the backups within 35 days
End of contract	Within 30 days	Returned, deleted or both, as you choose, with a deletion certificate

10. Sub-processors

Sub-processor	What it does	Where
Microsoft Ireland Operations Ltd (Microsoft Azure)	Hosting, database, backups, key management, logging	UK South
Amazon Web Services EMEA SARL (Amazon Bedrock)	Runs the AI model on extracts of plan text and, only where AI analysis in review preparation is on (off for real pupil data), on filtered review evidence	London (eu-west-2)
Amazon Web Services EMEA SARL (Amazon SES)	Email to staff, such as invitations. No pupil data	London (eu-west-2)

Sendix gives at least 30 days' written notice before adding or replacing a sub-processor, and you can object (DPA clause 5.2).

11. Top residual risks (after mitigation)

Scored Likelihood (1–5) × Severity (1–5): **1–3 Low, 4–6 Medium, 7 and above High**. The DPIA rates each risk in words; the scores are Sendix's assessment, mapping Remote, Possible and Probable to 1, 2 and 3, and Minimal, Significant and Severe to 1, 2 and 3. Every score falls in the level the DPIA gives.

Sendix AI Ltd · SC883770 · registered in Scotland · ICO ZC264381 · privacy@sendix.ai

Risk	Residual (L×S)	Level
R1 An external attacker reads plan text (independent penetration test pending)	2 × 3 = 6	**Medium**
R4 A child is re-identified from stored text	2 × 2 = 4	**Medium**
R6 A wrong suggestion is relied on	2 × 2 = 4	**Medium**
R21 Real data is added to a demonstration organisation	2 × 3 = 6	**Medium**
R33 A report about another child is added to a review	2 × 3 = 6	**Medium**
R2 A user at another school reaches your plans	1 × 3 = 3	Low
R3 A Sendix administrator reaches plan text	1 × 3 = 3	Low

The controller owns acceptance. Each controller decides in its own DPIA whether to accept these risks. The Key Risks and Mitigations register lists the rest. R30 would be High if AI analysis were on for real pupil data, which is why it stays off.

Pilot rule. Until the independent penetration test is complete, Sendix releases live pupil data to **no more than 3 organisations in total** (schools, trusts and alternative provision all count). An organisation is released only when Sendix holds a current Cyber Essentials certificate, the cross-school isolation tests pass on the version in production, the DPA is signed by both parties, and the controller's DPO has accepted R1 and R4 in writing. Until then, only fictional plans are used.

12. Further documentation and contact

- **Onboarding:** Data Processing Agreement v1.4; DPIA templates for academy trusts, maintained schools, independent schools and Scottish councils; Key Risks and Mitigations; Compliance FAQs.
- **Assurance:** Security Overview; sub-processors; infrastructure and break-glass access; breach notice; exit and continuity; DfE generative AI product safety self-assessment.
- **On request:** Sendix's DPIA (v0.7).

Contact: Sendix's Data Protection Lead, privacy@sendix.ai. Please don't send pupil information by email.

Sendix AI Ltd · SC883770 · registered in Scotland · ICO ZC264381 · privacy@sendix.ai