Key Risks and Mitigations

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

The risks in Sendix's own DPIA, what Sendix does about each, and the risk that remains. **Each controller accepts residual risk in its own DPIA**: this register is the processor's view, to help your DPO complete theirs.

Scoring. Likelihood (1–5) × Severity (1–5) after mitigation: **1–3 Low, 4–6 Medium, 7 and above High**. The DPIA rates likelihood as Remote, Possible or Probable and severity as Minimal, Significant or Severe; as Sendix's assessment, these map to 1, 2 and 3 on each scale, and every score falls in the level the DPIA gives. With AI analysis off, no risk is rated High. R30 would be High if analysis were on for real pupil data, which is why it stays off. Ratings for R27 to R29 are targets, because that feature is not built.

Risk	Category	Key mitigations	Residual (L×S)
R1 An external attacker reads plan text	Security	Signed-in access only, checked per school; MFA for SENCOs, SEND leads and Sendix administrators; lockout and rate limits; TLS and encryption at rest; enforced security headers; scanning on every change and weekly. 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: booked for January 2027, complete before a fourth. Until it is complete, the pilot rule applies (no more than 3 organisations, each released only with a Cyber Essentials certificate, isolation tests passing on the production version, and its DPO's written acceptance of this risk)	2 × 3 = 6 **Medium**
R2 A user at another school or trust reaches your plans	Access	Plans belong to the school; one access policy for every plan route; access ends when someone leaves; cross-school isolation tests on every change, and a build that leaks does not ship	1 × 3 = 3 Low
R3 A Sendix administrator reaches plan text	Access	Administrators cannot open plan text in the application, and there is no impersonation feature; data requests are handled by reference, and your staff download exports themselves; you are emailed whenever plans are handed to another member of your staff; MFA; role changes audit-logged. One person (the founder) holds infrastructure access, with MFA; individual database queries are not logged	1 × 3 = 3 Low
R4 A child is re-identified from stored text	Minimisation	Name and recognised identifier patterns removed before storage, or the upload is refused; EHCP sections C, D, G and H discarded on plan-ingestion paths; LA case references in text are not generally removed; other people's names replaced with roles (best-effort); visible only to the school's plan staff; bounded retention. A rare need or a placement name can still point to a child. Your DPO accepts this risk in writing before release	2 × 2 = 4 **Medium**
R5 The AI provider keeps or reuses data	AI	Amazon Bedrock in London, in-region only; fail-closed model approval; no storage of prompts or outputs and no training, under the provider's terms	1 × 2 = 2 Low
R6 A wrong suggestion is relied on	AI	Every plan wording suggestion accepted, edited or rejected by staff; only accepted plan wording changes exported; each finding cites its basis; suggestions use only evidence in the plan; a permanent notice that suggestions can be wrong and are not legal advice. Still to do: an accuracy evaluation on fictional plans before live use	2 × 2 = 4 **Medium**

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

R7 Data is kept too long	Retention	Daily deletion job with per-organisation periods and a dry-run preview, running since 3 October 2026; backups overwritten within 35 days; offboarding with a deletion certificate	1 × 2 = 2 Low
R8 A rights request is not met in time	Rights	Per-plan export, erasure and restriction; a runbook with the DPA's deadlines (forwarded within 5 working days, actioned within 10)	1 × 2 = 2 Low
R9 Personal data in logs	Security	Query strings stripped; a test blocks sensitive values in log calls; logs in UK South, kept 30 days	1 × 2 = 2 Low
R10 Test systems expose production data	Security	Separate staging database; build systems never receive production database credentials	1 × 3 = 3 Low
R11 Data is used for another purpose	Governance	No analytics or training pipeline; the DPA prohibits secondary use; any new use needs a DPIA update	1 × 2 = 2 Low
R12 Data is lost	Resilience	Automated backups for 35 days in UK South. Still to do: a tested restore before the first organisation is released	1 × 2 = 2 Low
R13 An account is taken over by password guessing	Security	Lockout after 5 failures; per-IP limits; deny-list; MFA for SENCO, SEND lead and administrator accounts	1 × 2 = 2 Low
R14 Data is transferred outside the UK	Transfers	Application, data, logs and AI model all in the UK. GitHub and Cloudflare hold no personal data; the public website, which holds no pupil data, is served from Azure West Europe	1 × 1 = 1 Low
R15 Name hashes are reversed or the key is exposed (delivery routes)	Security	Keyed per school; no fallback key; the persistent hash is opt-in per school; pending rows deleted after 30 days	2 × 2 = 4 **Medium**
R16 An import attaches a record to the wrong child (delivery routes)	Accuracy	Exact matching by UPN or LA reference; a name match is only a suggestion a SENCO confirms; imports never overwrite staff records	2 × 2 = 4 **Medium**
R17 An export reaches the wrong person or carries too much (delivery routes)	Disclosure	Allow-listed blocks with roles and dates; optional named approval; downloads audit-logged; Sendix sends nothing	2 × 2 = 4 **Medium**
R18 A calendar feed address is shared (delivery routes)	Security	Token stored as a fingerprint; revocable; a per-organisation off switch; the Sendix reference by default; 180-day default expiry; events name no child	2 × 2 = 4 **Medium**
R19 Legal holds keep records too long, or an erasure is wrongly refused (delivery routes)	Rights	Erasure pauses held plans only; your DPO confirms, verified by call-back; offboarding is capped by DPA clause 8.3. You review each hold at least once a term; the app prompts at 365 days	2 × 2 = 4 **Medium**
R20 A SEND assistant sees more than assigned plans (delivery routes)	Access	Deny by default, tested route by route; assigned plans only, Section F and this term's records only; MFA	1 × 2 = 2 Low
R21 Real data is added to a demonstration organisation	Governance	A demo cannot be released for real data; a permanent "Fictional data only" banner; an attestation on each upload; uploads not made by Sendix's set-up deleted after 30 days	2 × 3 = 6 **Medium**
R27 A breach links a named child to their needs (pupil display names; not built)	Security	Planned: separate table and key; off by default, switched on per school; shortest usable name; each school's DPO accepts this in writing	Target 2 × 3 = 6 **Medium**

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

R28 The name reaches the AI model or a log (pupil display names; not built)	AI	Planned: the model never receives the name; a fail-closed check before every model call; log tests	Target 1 × 3 = 3 Low
R29 The wrong name is attached to a plan (pupil display names; not built)	Accuracy	Planned: staff confirm before storage; attributed correction	Target 1 × 2 = 2 Low
R30 AI misjudges progress or misses contrary evidence (review preparation)	AI	Analysis is off for real pupil data, until the founder records a release decision after an evaluation labelled by a SENCO. Staff record their own status and reason; a suggested status never reaches the write-up	Off: no exposure on real data. If on: 3 × 3 = 9 **High**
R31 Staff over-rely on AI (review preparation)	AI	The decision form starts blank; suggestions are kept apart from decisions. Staff must actively select a quote the model found before it reaches the write-up, a requirement in force before release	Off: no exposure on real data. If on: 2 × 2 = 4 **Medium**
R32 Staff knowledge holds third-party data (review preparation)	Minimisation	Filter on every entry; other names removed best-effort; encryption; staff can delete a passage	2 × 2 = 4 **Medium**
R33 A report about another child is added to a review (review preparation)	Accuracy	A labelled name must match the name staff typed; staff read parent and child views; staff can delete a document	2 × 3 = 6 **Medium**
R34 Reports hold more than the review needs (review preparation)	Minimisation	Reports are kept whole, and staff are told to add only what the review needs; encryption; evidence text deleted after 30 or 180 days where enforcement is on	2 × 2 = 4 **Medium**
R35 Instructions in a report steer the model (review preparation)	AI	Passages treated as data; fixed reply format; exact quote and citation checks; staff decide	Off: no exposure on real data. If on: 2 × 2 = 4 **Medium**
R36 A feature is switched on outside its gates (review preparation)	Governance	All switches default off. The global bypass stays false and is being removed, and a per-organisation analysis switch is added before analysis goes on	1 × 3 = 3 Low

What the controller does. Record your own measures (privacy notice, Appropriate Policy Document, retention period, staff briefing) and your residual risk ratings in your DPIA. Under the pilot rule your DPO accepts R1 and R4 in writing before your real data goes in. If your assessment leaves any risk High, consult the ICO first (UK GDPR Article 36).

Questions: privacy@sendix.ai.

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