Security Overview

Sendix · Based on DPA v1.4 Schedules 2 and 3 and DPIA v0.7 · November 2026

How Sendix protects plan data, who could reach it, and what has and has not been independently checked. It brings together the infrastructure and break-glass statement and the sub-processor list, which stay in this pack as separate documents with the detail.

1. Status at a glance

Item	Status
Cyber Essentials	Applied for on 9 October 2026 through IASME. The assessment is under way; no certificate has been issued.
Cyber Essentials Plus	Not started. After the independent penetration test
Independent penetration test	**Not yet done.** Booked for January 2027, and complete before a fourth is released. Scope: cross-school access and the release checks
Cross-school isolation tests	Run on every change; a build that leaks does not ship
Multi-factor authentication	Mandatory for Sendix administrators and for SENCO and SEND lead accounts
Breach notice	Within 24 hours (DPA clause 7.1)
Hosting	Microsoft Azure UK South; AI on Amazon Bedrock, AWS London (eu-west-2), with no retention or training
Scheduled deletion	Running since 3 October 2026; backups overwritten within 35 days

2. The pilot rule: before the penetration test

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. Sendix releases an organisation only when all of these are in place for it:

- both parties have signed the DPA (v1.4 or later), signed for the organisation by the controller's authorised officer;
- Sendix holds a **current Cyber Essentials certificate**, and gives its number in the release confirmation;
- the **cross-school isolation tests pass** on the version in production;
- the controller's **DPO has accepted in writing** the residual risks R1 (external attack, with the penetration test's booked date stated) and R4 (re-identification from stored text, Medium);
- Sendix confirms in writing that live data is released for that organisation only, with a release reference.

When the test is complete, Sendix shares its summary with each controller. No fourth organisation is released until it is. This rule is in DPA v1.4 Schedule 2 and DPIA v0.7, both approved on 6 November 2026.

3. Where data lives and what is kept

- **Microsoft Azure UK South:** the application, PostgreSQL database, secrets (Azure Key Vault), logs and backups. Backups are kept for 35 days, in UK South only.
- **Amazon Bedrock, AWS London (eu-west-2):** the AI model, called in-region by its direct model ID. Cross-region routes are refused in code.
- **Before storage,** the pupil's name, UPNs, NHS numbers, postcodes and most written dates are removed from plan text; on plan-ingestion paths EHCP sections C, D, G and H are discarded; other people's

names are replaced with roles, best-effort. LA case references in text are not generally removed.

- **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.
- **The original file is not kept.** Uploads are read in memory.
- **Encryption:** in transit with TLS; at rest with Azure platform encryption using Microsoft-managed keys. LA case references, UPNs and review preparation text also have field-level encryption. Plan text is not encrypted with a separate key held by your school, so anyone with administrative access to the database could read it (section 5).

4. In the application

- **Plans belong to the school.** Its SENCOs and SEND leads, and its trust's SEND lead, can see plan text, while the contracting organisation has a countersigned DPA. The member of staff who uploaded a plan keeps access while they remain a member of the school or trust, subject to each route's role and DPA checks. Leavers lose access, including to plans they uploaded. IT leads, billing administrators and other schools cannot see plan text.
- **Sendix administrators cannot open plan text,** findings, file names or pupil identifiers. There is no "log in as a user" feature. Data requests are handled by reference, and your staff download exports themselves.
- **Sign-in:** passwords of at least 12 characters, checked against a deny-list; lockout after 5 failed attempts; rate limits; sessions end after 30 minutes idle and are revoked on password reset, sign-out or role change. Single sign-on is not available.
- **Application security:** strict security headers and an enforced content security policy; dependencies, container images and code history scanned for vulnerabilities and secrets on every change and weekly, with high and critical fixes applied within 14 days; personal data excluded from application logs; a separate staging database; build systems never receive production database credentials.
- **Audit log** of role changes, lockouts, MFA events, data exports and plan hand-overs. Your billing administrators and SEND leads are emailed whenever Sendix hands plans to another member of your staff.
- **Per-organisation pause:** Sendix can stop new uploads and analyses for your organisation without ending the agreement. Existing plans stay readable and exportable.

5. Underneath the application

- **One person at Sendix, the founder,** holds administrative access to the Azure subscription, with MFA. That access includes the database and the key vault holding its password. No one else at Sendix has system access, and no contractors, advisers or support agents have access.
- **The deployment pipeline** (GitHub Actions) can deploy to the Azure resources. It runs tested code and is not used to query data.
- **The network.** The database is not on a private network. Its firewall accepts connections from services hosted in Azure, and every connection needs the database password and an encrypted connection.
- **What is recorded.** Every database job run and every change to Azure resources is in Azure's activity log, kept for 90 days. **Individual database queries are not logged.**
- **Break-glass** is used only when an administrator has lost their authenticator and no other administrator is available. It resets that person's MFA after a phone identity check, with the reason recorded. It does not read plan text.

6. Sub-processors

Sub-processor	What it does	Where

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

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. No pupil data	London (eu-west-2)

The AI model is Qwen3-235B-A22B-2507, an open-weight model, Bedrock model ID `qwen.qwen3-235b-a22b-2507-v1:0`, in-region on-demand. A model request is sent only if a current, signed approval record matches the exact endpoint, region and model ID; anything else is blocked. Bedrock does not store prompts or outputs for this model or use them for training.

Suppliers that never receive pupil data: Azure Static Web Apps (the public website, West Europe), Microsoft 365 (Sendix staff email), GitHub (code and deployment) and Cloudflare (DNS). Sendix gives at least 30 days' notice of any new sub-processor, and you can object (DPA clause 5.2).

7. Incidents

If a personal data breach affects your data, Sendix tells you without undue delay, and in any event within 24 hours of becoming aware of it, and helps you decide whether to report to the ICO and tell families (DPA clause 7). To report a concern, email privacy@sendix.ai with "Security" in the subject line. Please don't include pupil information.

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