Infrastructure and break-glass access

Sendix · For school, trust and Scottish council DPOs · based on DPA v1.4 and DPIA v0.7 · November 2026

This replaces the shorter line "Sendix administrators cannot see plan text, through the application". That line is true, but it only covers the application. This page also covers the infrastructure underneath it.

1. Inside the Sendix application

- A Sendix administrator account cannot open plan text, extracted clauses, findings, file names, pupil identifiers, follow-through notes, IEP review records or review preparation records. The check is in the code that serves every plan, and an administrator gets "not found", even if the account also has a school role.
- Automated tests run in every build. They try each protected route as an administrator and as staff from another school, trust or role. A build that leaks data does not ship.
- There is no "log in as a user" or impersonation feature.
- Help with data requests uses metadata (dates, counts, references), not content. Your own staff download each plan's data export themselves.
- Two narrow cases: anyone signed in can open the fictional demonstration plans, and a Sendix staff member can open a plan they uploaded themselves (we upload only fictional plans).

2. Underneath the application

- **Where it is stored.** Plan extracts are kept in a PostgreSQL database in Microsoft Azure UK South. Before storage, the pupil's name, UPNs, NHS numbers, postcodes and most written dates are removed from the plan text, and on plan-ingestion paths the EHCP health and social care sections (C, D, G and H) are discarded. Other people's names are replaced with their role or relationship where the text makes that clear; this is best-effort.
- **Identifiers your school stores (delivery routes, not yet available for real pupil data).** If your school switches on delivery routes, the LA case reference and, optionally, the UPN are stored in the same database, apart from the plan text, encrypted at field level, together with keyed hashes of names used to match your own spreadsheets. Someone who could reach both the database and the key vault could read the references. The hashes can only be tested against a guessed name with a separate secret held in the key vault (`TRACKER_MATCH_SECRET`; see Sendix's key custody procedure, available on request).
- **Review preparation evidence (optional, England).** Reports, views and staff knowledge are stored whole, filtered but with no section discard, and are encrypted at field level under a key held in the key vault. Someone who could reach both the database and the key vault could read them.
- **How it is encrypted.** In transit with TLS, and at rest with Azure storage 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. Anyone with administrative access to the database could read it.
- **The original file is not kept.** Uploads are read in memory. For the "export to your own Word document" feature, your browser keeps an encrypted copy; our server holds only a fingerprint and a wrapped key.
- **Backups** are kept for 35 days, in UK South only.

3. Who could technically reach the database

- **One person at Sendix, the founder,** holds administrative access to the Azure subscription. No one else at Sendix has system access; the minority shareholder has none. That access includes the database and the key vault that holds its password. Azure sign-in for these accounts requires multi-factor

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

authentication.

- **Our deployment pipeline** (GitHub Actions) holds deployment rights to the Azure resources so that it can release new versions. It runs our tested code; it is not used to query data.
- **No one else**: no contractors, advisers or support agents have access.
- **The network.** The database is not on a private network. Its firewall accepts connections from any service hosted in Azure, not only Sendix's, and every connection needs the database password and an encrypted connection.

4. What we do and do not do with that access

- We do not read plan text. Our support and data-request procedures don't require it: requests are handled by reference, and your staff export content themselves.
- Database changes run inside Azure through a dedicated job, so the database password never leaves Azure. The job is set up to run only database migrations, setup scripts for fictional demo accounts, a read-only retention preview, and the break-glass reset below. That list guards against mistakes; it is not a security boundary. Someone with administrative access could change the job, or read the password from the key vault and connect to the database directly, and that connection would not be logged query by query.
- **Break-glass** is used only when a Sendix administrator has lost their authenticator and no other administrator is available. It resets that person's multi-factor authentication, after their identity has been checked by phone, with the reason recorded. It does not read plan text.

5. What is recorded

- Every run of the database job, and every change to Azure resources, appears in Azure's job history and activity log, with who started it. Azure keeps the activity log for 90 days.
- The application's audit log records role changes, lockouts, MFA events, exports and plan hand-overs.
- **Individual database queries are not logged.** If someone with administrative access read the database directly, that read would not be recorded query by query.

6. Bringing your own questions

Email privacy@sendix.ai. Please don't send pupil information by email. The independent penetration test (not yet done; booked for January 2027; until it is complete, no more than 3 organisations use real plans) will cover cross-school access and the release checks; we share its summary with each school before its real plans are uploaded.

Review status: approved by Sendix (Data Protection Lead), 6 November 2026, after AI-assisted legal and data protection review; independent solicitor and DPO review scheduled as Sendix scales.

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