

Data Protection

A summary of the data The SENDNest for Schools holds, where it is stored and how it is protected.

PUPIL DATA

The platform holds **no pupil data**. Staff work with general, non-identifying professional content: the needs, barriers, outcomes and strategies of the graduated approach. A pupil's name is added on the school's own screen when a document is exported, and it is never sent to us or to the drafting provider.

What we do hold

Staff and school data only:

- Staff accounts: name, work email, role
- Training progress, scores and certificates
- The school-level inputs to your SEND information report (provision, links and dates, never individual pupil information)
- Technical and security records any service keeps, such as sign-in events

Your school is the data controller for this. The SENDNest for Schools is your processor under a signed Data Processing Agreement.

Where it is stored

In the United Kingdom. Your data sits at rest with Supabase on Amazon Web Services in London (region eu-west-2). Row-level security separates every school's data, and every role within it, from every other. Some of the providers below may process limited data outside the United Kingdom, always under the approved transfer safeguards set out in our Data Processing Agreement.

Sub-processors

Supabase	Secure database and sign-in, in the United Kingdom (AWS London).
Netlify	Hosting and delivery of the application.
Cloudflare Stream	Training video, served through signed, expiring links.
Resend	System emails, such as your sign-in link and welcome message.

Each is engaged under its own data processing agreement with recognised UK transfer safeguards. Drafting is assisted by **Anthropic's API**, which receives only the non-identifying needs and strategy content: never a pupil's identity, your staff data, or your working files. Anthropic is named here for transparency and is not appointed to process personal data. Its API content is not used to train models and is deleted from its systems within 30 days, subject to the limited exceptions described in our Privacy Notice.

Security

- Sign-in by emailed link; no passwords are used
- Encryption in transit and at rest
- Row-level isolation between schools and roles
- Minimised logging: no draft content, generated text or pupil identity is intentionally recorded; we keep only the security records a service needs, such as sign-in events
- Automated security and integrity checks run before every change we release

When a subscription ends

When a subscription ends, the school has 30 days to export what it needs. After that period we delete the staff accounts and training records we hold from our live systems, and from backups as they cycle. Exported documents are held in the school's own systems.

DOCUMENTS

Available for review: our **Data Processing Agreement** and **Privacy Notice**, a platform **Data Protection Impact Assessment** completed to the standard the law expects of a mandatory one, and our **incident-response** and **complaints** procedures. If a personal data breach affects your data, we tell you without undue delay and help you meet your own reporting duties, including any report to the Information Commissioner's Office within 72 hours. The company will hold professional indemnity insurance and complete its registration with the Information Commissioner's Office before it holds any school's data. This is a summary; the Data Processing Agreement and Privacy Notice hold the binding detail.