Data Protection Pack

for Data Protection Officers

Baobab — The complete system for SEND delivery

Provider	Baobab Education Ltd
Company number	17047934
Product	Baobab (app.baobab.education)
Contact	hello@baobab.education
Privacy policy	https://app.baobab.education/privacy

This pack contains the four standard documents required by a school's Data Protection Officer: a Data Processing Agreement (Article 28 UK GDPR), a statement of data storage locations, our security standards, and a register of sub-processors.

1. Data Processing Agreement

Article 28 UK GDPR — between Baobab Education Ltd (“Processor”) and the School (“Controller”).

Parties

Controller (School)	_____
	Address: _____
	Represented by: _____
Processor	Baobab Education Ltd
	Company No. 17047934, registered in England & Wales
	Represented by: Bryan Plumb, Founder
Effective date	____ / ____ / _____

1. Subject matter and duration

The Processor provides the Baobab platform to the Controller for the recording, tracking and reporting of Special Educational Needs and Disabilities (SEND) provision. Processing continues for the duration of the Controller’s subscription and any wind-down period set out in clause 11.

2. Nature and purpose of processing

The Processor processes personal data only to: (a) operate, secure and support the Baobab platform; (b) generate documents (e.g. EHCP delivery reports) requested by the Controller; and (c) provide AI-assisted features on pseudonymised data as set out in clause 6.

3. Categories of data subjects

Pupils with SEND (including those with EHCPs and those receiving SEN Support); school staff who use the platform (e.g. SENDCos, teachers, teaching assistants); parents/carers where named in EHCPs or progress notes.

4. Categories of personal data

Pupil identifiers (name, DOB, UPN, year group); educational records (EHCPs, outcomes, provisions, progress updates, supporting documents); special category data under Article 9 (health, SEN diagnoses, professional reports); staff account data (name, work email, role, audit events).

5. Controller instructions

The Processor shall process personal data only on the documented instructions of the Controller, including with regard to transfers to a third country, unless required to do so by law. This Agreement and the Controller’s use of the platform constitute the Controller’s documented instructions.

6. AI processing and pseudonymisation

Where AI features are used (e.g. EHCP extraction, report drafting, insights chat), the Processor pseudonymises pupil-identifying fields server-side before any data is sent to AI inference endpoints: pupil names are replaced with sequential labels (“Child A”, “Child B”), and DOBs/UPNs are stripped. AI providers receive no identifying data, do not retain inputs and do not train on Controller data.

7. Confidentiality

The Processor ensures that persons authorised to process the personal data are bound by confidentiality obligations and are trained on data protection.

8. Security (Article 32)

The Processor implements the technical and organisational measures set out in the “Security standards” section of this pack, including encryption at rest and in transit, mandatory two-factor authentication, Row-Level Security scoped by school, audit logging and breach response procedures.

9. Sub-processors

The Controller provides general written authorisation for the Processor to engage the sub-processors listed in the “Sub-processors register” section of this pack. The Processor shall inform the Controller of any intended changes and give the Controller the opportunity to object on reasonable data-protection grounds. The Processor shall impose equivalent data-protection obligations on every sub-processor.

10. Assistance to the Controller

Taking into account the nature of processing, the Processor shall assist the Controller, by appropriate technical and organisational measures and insofar as possible, in: (a) responding to requests from data subjects exercising their rights under Chapter III UK GDPR; (b) ensuring compliance with Articles 32–36 (security, breach notification, DPIAs and prior consultation).

11. Personal data breach

The Processor shall notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a personal data breach affecting the Controller’s data, providing the information required by Article 33(3).

12. Return or deletion

On termination of the services, and at the choice of the Controller, the Processor shall return or delete all personal data within 30 days, and delete existing copies unless storage is required by law. Backups containing the data shall be overwritten in the ordinary course within the documented backup retention period.

13. Audits and information

The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28, and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, on reasonable notice and subject to confidentiality.

14. International transfers

Identifiable pupil data is stored and processed within the UK/EEA. Where any limited transfer outside the UK/EEA is necessary (e.g. transactional email to staff addresses), the Processor relies on appropriate safeguards under Article 46 (including UK IDTA / Standard Contractual Clauses) and the UK Addendum.

15. Liability and governing law

This Agreement is governed by the laws of England and Wales. Liability is as set out in the parties’ underlying services agreement or, in its absence, as limited by law.

Signed for and on behalf of the parties

Controller (School)	**Processor (Baobab)**
Name: _____	Name: Bryan Plumb
Title: _____	Title: Founder
Organisation: _____	Organisation: Baobab Education Ltd (Co. No. 17047934)
Signature: _____	Signature: _____
Date: _____	Date: _____

2. Data storage locations

Where Baobab stores and processes Controller data.

Data category	Location	Provider
Primary database (Postgres)	EU — Frankfurt (eu-central-1)	Supabase / AWS
File storage (EHCPs, supporting docs, PDFs)	EU — Frankfurt (eu-central-1)	Supabase Storage / AWS S3
Backups (encrypted at rest)	EU — Frankfurt (eu-central-1)	Supabase / AWS
Edge functions (server-side logic)	EU region	Supabase Edge Functions
AI inference (pseudonymised text only)	EU inference endpoints	Lovable AI Gateway (Google / OpenAI)
Transactional email (staff only, no pupil data)	US	Resend
CRM lifecycle webhooks (staff contact only)	US	Zapier / LeadConnector

Key principles

- **Identifiable pupil data never leaves the UK/EEA.** All databases, file storage and backups are hosted in Frankfurt (eu-central-1).
- **AI processing is EU-region and pseudonymised.** Pupil names and identifiers are stripped server-side before any AI call; AI providers do not retain or train on Controller data.
- **US sub-processors receive staff-only data.** Resend (email) and Zapier (CRM webhooks) only ever receive staff contact information — never pupil data.
- **Transfer safeguards.** Any limited transfer outside the UK/EEA relies on UK IDTA / Standard Contractual Clauses with the relevant sub-processor.

3. Security standards

Technical and organisational measures under Article 32 UK GDPR.

Encryption

- AES-256 encryption at rest for databases, file storage and backups.
- TLS 1.2+ in transit for all client and server-to-server connections.
- Private storage buckets only — EHCP PDFs and supporting documents are never publicly accessible; access is via short-lived signed URLs.

Authentication & authorisation

- Mandatory two-factor authentication for every user via 6-digit email OTP.
- Platform admin panel separately MFA-gated with server-verified session tokens (SHA-256 hashed).
- Postgres Row-Level Security (RLS) scoped by **school_id** on every table; default-deny policies.
- Roles held in a separate **user_roles** table (not on profiles) to prevent privilege escalation; granular per-user permissions for contributors.
- Passwords hashed by Supabase Auth; HTTP-only session tokens; rate limiting on sensitive endpoints.

AI data protection

- Server-side pseudonymisation: pupil names → “Child A / B / C”; DOBs and UPNs stripped before any AI call.
- Reverse mapping happens server-side after the AI response; the AI provider only ever sees pseudonymised data.
- AI providers contractually do not train on, or retain, Controller inputs.

Audit & monitoring

- Audit log of significant actions (EHCP uploads, child created/archived, support access, role changes) retained for 6 years.
- Support access logged with explicit consent, ticket reference, and start/end timestamps; an “Admin mode” banner is displayed throughout.
- Real-time connectivity and error monitoring; React error boundaries with branded recovery surfaces.

Support access controls

- Per-ticket consent required — no standing access.
- Time-limited and MFA-gated for the supporting member of staff.
- No bulk export from support tooling; all access actions audited.

Breach response

- Documented incident response procedure.
- Notification to affected schools without undue delay and in any event within 72 hours of becoming aware of a personal data breach.
- Post-incident review and remediation tracked to closure.

4. Sub-processors register

Current as of the date of issue. Schools will be notified of material changes.

Sub-processor	Role	Location	Data received	Safeguards
Supabase (AWS)	Database, file storage, authentication, edge functions	EU (Frankfurt)	All school and pupil data	DPA in place; EU region; encryption at rest and in transit; RLS
Lovable AI Gateway (Google / OpenAI models)	AI extraction and content generation	EU inference	Pseudonymised text only	No PII sent; no training on Controller data; no retention
Resend	Transactional email (OTPs, invitations, notifications)	US	Staff email addresses only	DPA in place; no pupil data; UK IDTA / SCCs
Zapier / LeadConnector	CRM lifecycle webhooks	US	Staff contact details and lifecycle event metadata	No pupil data; UK IDTA / SCCs

Change notification

Baobab will notify the Controller of any intended addition or replacement of sub-processors with reasonable advance notice, giving the Controller the opportunity to object on reasonable data-protection grounds in accordance with clause 9 of the DPA.

For questions about this pack, contact **hello@baobab.education**. The current public privacy policy is available at **https://app.baobab.education/privacy**.