INTERNAL · FOR TBS EDUCATION LTD OY STAFF AND CONTRACTORS

Internal Data Policies

Operational policies for handling personal data · Effective 28 April 2026

ORGANISATION REGISTRATION

TBS Education Ltd Oy · Business ID 3614159-3 · Lahti, Finland
UK ICO Registration: ZC133810

1. SCOPE

This document describes the internal operational policies of TBS Education Ltd Oy with respect to personal data. It applies to all staff, founders, and engaged contractors. It supplements (and is consistent with) the public-facing Privacy Policy and the Data Processing Agreement signed with each customer school.

2. ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Data Protection Lead	Sakari Laajoki (Founder & Director) — first point of contact for all data-protection enquiries, breach response, and regulator correspondence.
Engineering Partner	Appifest, Sydney, Australia (Muhammad Feroz) — operates the production codebase under written confidentiality terms; access to production database is logged and audited.
Sub-processors	Netlify (frontend), Neon (database), Anthropic (AI inference). Each operates under their own DPA and Standard Contractual Clauses.

3. ACCESS CONTROL

- Production database access is limited to the Data Protection Lead and the contracted Engineering Partner
- Each access uses a uniquely identifiable credential; shared accounts are not permitted
- Multi-factor authentication is enabled on the Neon, Netlify and Anthropic admin consoles
- Access is reviewed quarterly; any contractor whose engagement ends has access revoked within 24 hours

4. DATA MINIMISATION

- The simulation collects only what is operationally necessary (see Privacy Policy section 3)
- No real student names, emails, dates of birth, addresses or photos are collected
- Students join via PIN code — no account or password is required or generated
- Free-tier session data is auto-deleted within 24 hours of session end

5. ENCRYPTION

- All connections use HTTPS / TLS 1.2 or higher
- The production database is encrypted at rest using AES-256
- Backups are encrypted and held by the database provider; encryption keys are managed by the provider

6. LOGGING AND MONITORING

- Server logs (including IP addresses) are retained for 30 days, then auto-purged
- Database admin actions are logged by Neon
- Application errors are surfaced to the Engineering Partner for investigation

7. BREACH RESPONSE

If a personal data breach is suspected or confirmed, the following process applies:

1. **Hour 0–2:** Containment — the Data Protection Lead and Engineering Partner isolate affected systems; access tokens are rotated
2. **Hour 2–24:** Assessment — scope, data categories, number of data subjects, and risk to rights and freedoms are documented
3. **Hour 24–72:** Notification — affected schools (Controllers) are notified within 72 hours of awareness, with all information required under UK GDPR Art. 33. The UK ICO and the Finnish Data Protection Ombudsman are notified directly where required
4. **Day 7:** Post-incident review — root cause, remediation, and policy updates are documented

The Data Protection Lead is Sakari Laajoki, sakari.laajoki@gmail.com.

8. SUB-PROCESSOR ENGAGEMENT

- New sub-processors are engaged only under a written DPA that mirrors the obligations in our customer DPA
- Each sub-processor's location, purpose and transfer safeguard is recorded in the public-facing Privacy Policy and DPA
- Customer schools are notified at least 30 days in advance of any new or replacement sub-processor

9. TRAINING AND AWARENESS

- The Data Protection Lead reviews UK GDPR, UK Data Protection Act 2018, and KCSIE 2024/25 §143 obligations annually
- Engineering Partner receives a written briefing on these obligations at the start of the engagement and on any material change
- Cyber Essentials Verified Self-Assessment is in progress with IASME

10. DATA SUBJECT RIGHTS — INTERNAL WORKFLOW

When a data-subject request is received (typically via the school as Controller):

1. Acknowledge within 5 working days

2. Verify identity (or rely on Controller verification)
3. Locate relevant records; redact third-party personal data
4. Respond within 30 days of receipt; in complex cases, extend to 60 days with written explanation
5. Log the request and response in the internal register

11. RETENTION AND DELETION

DATA TYPE	RETENTION	TRIGGER TO DELETE
Free-tier session data	≤ 24 hours	Session end + 24h auto-delete
Paid-tier saved sessions	Teacher-controlled	Teacher delete action
Teacher account data	Subscription duration	Subscription termination + 30 days
Server logs (incl. IP)	30 days	Auto-purge
Backups	30 days rolling	Auto-rotation

12. REVIEW

This document is reviewed at least annually by the Data Protection Lead, and immediately after any material change to processing, sub-processors, or applicable law.