Massachusetts Student Data Privacy Agreement – Exhibits A, B, F

Provider: ImagineAI LLC
Service: ImagineAI (student/teacher AI book-building)
Effective Date: November 24, 2025
Governing Law/Venue: Commonwealth of Massachusetts; Plymouth County courts

---

Exhibit A – Description of Services

ImagineAI provides a web application where teachers and students co-create illustrated books through conversational AI and image generation. Key functions:

- Teacher dashboard scoped to the teacher's own classes/students; classroom codes to invite students.
- Student workspace to chat with an AI assistant, generate text and images, and assemble book content.
- Hosting/Application: Railway/Heroku (US-only). Database/Auth: Supabase/PostgreSQL (US-only). Email: Resend (transactional). Generative models: OpenAI, Anthropic (text), Google image models, FAL.ai (image/video); prompts/outputs are processed transiently and not used for model training.
- No advertising, no analytics, no sale of data.

Exhibit B – Schedule of Data Collected/Processed

We collect only what is needed to operate the classroom service:

- Identifiers: teacher email; student username; optional student name as typed on a book title page; classroom code.
- Credentials: hashed password or federated auth tokens.
- Student work: generated text, images, and book content; class membership.
- System logs: minimal service logs (timestamps/error traces); no retained IP addresses beyond transient transport logs required by hosting providers.
- We do **not** collect: photos/voice/biometrics, precise geolocation, disability/IEP/ELL/race/ethnicity/socioeconomic flags, behavioral/discipline data, medical data, payment data, or advertising identifiers.

Exhibit F – Data Security Requirements

- **Policy/Framework:** Lightweight written controls documented here; encryption in transit (TLS) and at rest; least-privilege access.
- **Access Control:** Production data access limited to the founder/administrator; authenticated, logged access; confidentiality obligation applies.
- **Hosting/Region:** US-only (Railway/Heroku app hosting; Supabase/PostgreSQL data). No storage outside the United States.
- **Backups:** Supabase-managed automated backups/point-in-time recovery per Supabase retention; deletions propagate as retention windows expire.

- **Encryption:** TLS for data in transit; at-rest encryption provided by managed services (Supabase, hosting providers).
- **Authentication:** Passwords hashed; teacher/student auth via Supabase; optional OAuth for teachers.
- **Subprocessors (all US-only):** Supabase (DB/auth), Railway/Heroku (app), Resend (email), OpenAI/Anthropic (LLM generation), Google image models, FAL.ai (image/video generation). No analytics vendors.
- **Logging/Monitoring:** Minimal application logs (no persistent IP retention); error logs used for support/security.
- **Risk & Patching:** Periodic informal risk review; apply upstream security patches from providers.
- **Breach Response:** Notify LEA within 10 days of confirmed unauthorized access; cooperate with investigation; provide required details per MSPA.
- **Deletion/Return:** Upon LEA request, return specified Student Data within 3 days and delete as soon as practicable (target 3 days), with written confirmation.
- **Data Segregation:** Per-tenant scoping by classroom codes and role-based checks in the app.
- **Personnel:** Single-employee company; no background check program needed beyond founder; no other staff with production access.
- **Ads/Profiling:** None; Student Data not used for marketing or targeted advertising; no model training on Student Data.