ImagineAI LLC – Data Security & Privacy Plan (NIST CSF v1.1)

Scope: ImagineAI web app for classroom book creation (teachers/students). Single-employee company.
Effective: November 24, 2025.
Contact: Kyle Maloney (Founder/CEO) – kyle30683@gmail.com – 774-766-8131.
Plan URL: https://imagineai.one/data-security-privacy-plan.pdf

Data Minimization

- Student data: student email (for login only); student app username; optional student name (typed on book cover); classroom code; hashed password or federated auth token; student-generated content (text/images/books); per-student usage metrics (e.g., word/activity counts surfaced to the teacher); minimal app logs (timestamps/error traces); no persistent IP retention beyond transport/provider ephemeral logs.
- Teacher data: teacher email; teacher app username/password; teacher-generated content; minimal app logs.
- Not collected: photos/voice/biometrics; precise location; disability/IEP/ELL/race/ethnicity; behavior/discipline; health; payment data; advertising IDs; parent contact info; SSNs; IDs other than app username/password and student email; third-party analytics.

Subprocessors (US-only)

- Supabase (Postgres DB/auth; managed backups).
- Railway/Heroku (app hosting).
- Resend (transactional email to teachers).
- OpenAI, Anthropic (text generation; prompts/outputs transient; not used for training).
- Google image models; FAL.ai (image/video generation; transient; not used for training).

Security Framework and Controls (NIST CSF v1.1)

- Identify: inventory of data flows and subprocessors; single-employee access; US-only regions.
- Protect: TLS in transit; at-rest encryption via managed services; hashed passwords; least-privilege console access; no ads/marketing; privacy-by-default scopes by classroom; background check not applicable beyond founder (sole operator).
- Detect: minimal app/error logs; provider alerts from hosting/DB; manual review when anomalies occur.
- Respond: incident response playbook; notify LEA within 72 hours of confirmed incident (24h initial notice if required, e.g., VA); include required details; cooperate with LEA and law enforcement; preserve logs.
- Recover: rely on Supabase managed backups/PITR; restore from snapshots; post-incident lessons learned and patching.

Access, Authentication, and Handling

- Single-employee production access; MFA on provider consoles; confidentiality obligation applies.
- Role-based app access: teachers limited to their classes; students limited to own work; classroom codes for join flow.
- No data use for advertising or profiling; no model training on Student Data; subprocessors bound to equivalent protections.

Retention & Deletion

- Keep data while classroom is active; upon LEA request return data within 3 days and delete as soon as practicable (target 3 days) with confirmation; deletions propagate as Supabase backup retention windows expire.
- De-identified data may be retained for service improvement without re-identification.

Training & Governance

- Founder/CEO performs security/privacy responsibilities; annual policy review; updates subprocessors list and notifies LEAs before changes.
- References: FERPA, COPPA, state addenda in NDPA, NY Ed Law 2-d; NIST CSF baseline.

Incident/Breach Response

- Notify LEA within 72 hours of confirmed unauthorized access; earlier if required by state (e.g., 24h VA).
- Notification includes required elements (type, date/range, count if known, contact, description, law enforcement delay if applicable).
- Cooperate on investigation, containment, remediation, and notifications.

Student/Parent Rights

- Upon LEA request, provide/correct Student Data within required timeframe; refer direct parent/student inquiries to LEA and cooperate.

Contact

- Kyle Maloney – Founder/CEO

  kyle30683@gmail.com | 774-766-8131
  5 Applewood Ct, Bourne, MA 02532