Data Processing Agreement

Between: Your School / District ("Controller") and CyberHeroesHQ, operated by Polsia, Inc. ("Processor")

Effective Date: _____

Term: Co-terminus with the master subscription or pilot agreement.

Jurisdiction: United States; state law supplement where applicable to the Controller's jurisdiction.

1. Parties and Purpose

This Data Processing Agreement ("DPA") supplements any order form, pilot agreement, or terms of service between the Controller (the school or district) and Processor (CyberHeroesHQ / Polsia, Inc.) and governs how Processor handles Student Personal Information collected through the CyberHeroesHQ platform.

Processor operates the CyberHeroesHQ cybersecurity education platform ("Platform"), a K–12 curriculum delivery and assessment service. Processor processes Student Personal Information strictly on behalf of the Controller for the educational purpose defined in the underlying subscription, pilot, or master agreement.

2. FERPA School Official Exception

Processor agrees: (a) it has been designated a "school official" with a legitimate educational interest under FERPA (34 C.F.R. § 99.31(a)(1)); (b) it will use Student Personal Information only to perform services specified herein and for no other commercial purpose; (c) it will comply with FERPA in the same manner as the Controller as an institution; and (d) it will not disclose Student Personal Information to any third party without prior written consent of the Controller, except as required by law or to a subprocessor with a signed DPA.

Processor does not condition educational service delivery on a parent or eligible student's waiver of FERPA rights, and does not use Student Personal Information for advertising, profiling, or any commercial purpose.

3. COPPA Compliance and Parental Consent

Processor does not knowingly collect personal information from children under 13 without verifiable parental consent obtained by the Controller. The Controller, by creating student accounts via classroom codes issued by teachers, represents that it has the authority to consent on behalf of parents under the COPPA school authorization mechanism (16 C.F.R. § 312.5(b)(1)).

For Family Plan consumers (parents creating home accounts), Processor obtains affirmative COPPA consent at account creation via an explicit consent checkbox, and provides a parent dashboard with view, export, and deletion tools as further described in Section 12 (Data Subject Rights).

4. Categories of Student Personal Information Processed

Processor processes the following categories of Student Personal Information solely to deliver the Platform:

- Hero username (chosen by student or assigned by teacher — never legal name)
- Mission progress, quiz scores, badges unlocked, XP earned
- Pre- and post-assessment results (topic-level; not personally identifiable outside the classroom)
- Classroom identifier (links student to the teacher dashboard only)
- Session data (IP address, browser type — transient, retained "d 7 days)
- Parent email (opt-in only, used for the family-plan weekly digest)

We explicitly DO NOT collect:

- Legal name, date of birth, or government-issued identifiers

- Physical location (GPS, precise address, school address linked to student)
- Biometric data of any kind
- Behavioral advertising profiles or cross-context tracking signals
- Health, disability, or financial information
- Social Security numbers or government benefits identifiers

5. Subprocessors

Processor engages the subprocessors listed below to deliver the Platform. Each operates under a signed DPA, processes data only for the stated purpose, and is bound by confidentiality and security commitments materially equivalent to those in this agreement. Processor will notify Controller of any new subprocessor at least 30 days in advance.

Neon (database)
Purpose: PostgreSQL database hosting (AES-256 at rest, AWS-managed KMS). Data region: US East (AWS).

Render
Purpose: Application hosting and deployment. Data region: US (Oregon).

Postmark
Purpose: Transactional email (parent and teacher notifications). Data region: US.

Stripe
Purpose: Payment processing (no student data shared; PCI-DSS L1). Data region: US.

OpenAI
Purpose: AI-generated daily challenge content (no PII in prompts). Data region: US.

Anthropic (Claude)
Purpose: Cipher AI mentor (session-scoped, no PII, no training). Data region: US.

Google (OAuth only)
Purpose: Teacher/parent sign-in via OAuth — no student data flows. Data region: US.

Cloudflare
Purpose: Edge CDN and WAF (TLS 1.2+ termination; no PII stored). Data region: US edge.

6. International Data Transfers

Processor stores and processes all Student Personal Information inside the United States. No data is transferred to or stored in jurisdictions outside the United States without prior written consent of the Controller. For Controllers bound by GDPR-K or equivalent cross-border rules, Processor maintains a data-flow diagram and a current subprocessor list at /trust and as Annex I to this DPA.

7. Annex II — Technical and Organizational Security Measures

Processor implements and maintains the following technical and organizational security measures (Annex II, GDPR Art. 32 equivalent), continuously verified:

Encryption in transit.
TLS 1.2+ enforced on every public endpoint. HSTS preloaded. HTTP requests 301-redirected to HTTPS.

Encryption at rest.
AES-256 on all database storage via AWS KMS (managed keys). Backups encrypted with rotating keys; 35-day retention.

Password storage.
bcrypt at cost "e 12 for all user credentials. Session cookies are HttpOnly, Secure, SameSite=Lax.

Production access.
Multi-factor authentication required for all production database and deployment access. Access logged and reviewed.

Application monitoring.
Sentry error tracking with 20% trace sample in production; 100% capture of unhandled exceptions and promise rejections.

Uptime monitoring.

Better Stack external HTTP probes on /api/health every 60 seconds. Combined weekly infrastructure digest (Sunday 9am UTC).

Query safety.
100% parameterized SQL — no string interpolation in queries. Static check runs on every deploy.

Dependency hygiene.
npm audit on every deploy; critical and high vulnerabilities block deploy. Lockfile-pinned dependencies.

Backup posture.
Daily encrypted backups with 35-day retention. Continuous WAL via Neon. RTO < 4 hours, RPO < 5 minutes.

Penetration testing.
Annual third-party pen test against production. Findings tracked to remediation in the public Hall of Fame.

8. Breach Notification and Incident Response

Processor will notify the affected Controller (via the Controller's designated security contact, with copy to the district CIO/IT lead where on file) within 72 hours of becoming aware of a confirmed security incident involving Student Personal Information. Notification will include, to the extent known: the nature of the incident, the categories and approximate number of records affected, the likely consequences, and the measures taken or proposed to address the incident and mitigate adverse effects.

Processor cooperates with the Controller on regulatory notifications (state breach notification statutes, attorney general reporting) and on communications to affected families where the Controller desires to lead such communications.

9. Data Subject Rights and Parental Requests

Processor supports the Controller in responding to parent and eligible-student requests under FERPA, COPPA, and applicable state student-privacy laws. Parents may submit requests directly to privacy@cyberheroeshq.com; Processor will acknowledge within 5 business days and complete identity-verified requests within 45 days (30 days where required by state law).

- View: Parents may download a JSON export of their child's data from the Family Dashboard at /parent/family-dashboard.
- Correct: Teachers may correct hero name, classroom, and grade band in the Teacher Portal. Direct requests go to privacy@cyberheroeshq.com.
- Delete: Soft delete is available to parents in the Family Dashboard. Hard delete is performed within 30 days of verified written request.
- Revoke consent: Cancel subscription and email privacy@cyberheroeshq.com to confirm.

10. Retention, Soft Delete, and Hard Purge

Active subscriptions: Student Personal Information is retained for the term of the subscription plus a 90-day export grace period, during which the Controller may export data via the Teacher Portal or the Family Dashboard.

Soft delete (30-day grace): After account closure or pilot end, data is soft-deleted for 30 days. During this window the Controller may restore the classroom no questions asked.

Hard purge: All Student Personal Information is purged from primary, replica, and backup storage within 30 days of a written Controller request or the end of the soft-delete window, whichever comes first. Confirmed by written acknowledgement from Processor.

11. Audit Rights

Pre-attestation (current state): Until the SOC 2 Type 2 report described in Section 14 is delivered, Controller may, on 30 days' written notice and not more than once per calendar year, request an on-site or remote review of Processor's documentation of the controls listed in Section 7 (Annex II). Review will be at Controller's expense and subject to confidentiality protections.

Post-attestation: Following delivery of the SOC 2 Type 2 report, the report itself constitutes the primary audit artefact. Processor will make the report available to contracting Controllers under NDA on request.

Security questionnaires: Processor responds to HECVAT, SIG, and equivalent custom questionnaires within 5 business days of receipt. Contact security@cyberheroeshq.com.

12. Term, Termination, and Post-Termination Duties

This DPA is effective on the Effective Date set out above and remains in effect for the term of the underlying subscription, pilot, or master agreement (co-terminus).

Upon termination (for any reason): (a) Processor provides a 30-day window during which the Controller may export data via the standard export tools; (b) on the earlier of the Controller's written request or the end of that 30-day window, Processor performs a hard purge as described in Section 10; (c) obligations of confidentiality and security survive termination.

13. Governing Law and Disputes

This DPA is governed by the laws of the State of Delaware, without regard to conflict-of-laws principles. Disputes are resolved via good-faith negotiation followed, if necessary, by binding arbitration in Delaware. Nothing in this section limits a Controller's rights under FERPA, COPPA, or applicable state student-privacy law.

14. Independent Assurance — SOC 2 Roadmap

Currently pre-audit. Processor targets SOC 2 Type 1 in Q4 2026 and Type 2 in Q4 2027, in each case under AICPA Trust Services Criteria. Until the Type 2 report is delivered, Processor does not claim certified status; the controls listed in Section 7 are the same controls that will be in audit scope. The /trust page is updated first when any report is delivered.

15. Acceptance and Counter-Signature

This DPA becomes effective on the Effective Date and applies to all Student Personal Information processed by Processor on behalf of the Controller. The parties below acknowledge and accept the obligations set forth herein.

For a countersigned PDF, please return a signed copy to trust@cyberheroeshq.com. Email-only acceptance (per the underlying Terms of Service) is also recognized.

SCHOOL / DISTRICT (Controller)

_____
Authorized Signature

District Name: _____
Authorized Signatory: _____
Title: _____
Effective Date: _____

CYBERHEROES HQ / POLSIA, INC. (Processor)

_____
Authorized Signature / Date

Signatory: _____
Title: _____
Date: _____

Printable-fillable variant — fill by hand or use Adobe Editor. Email a scanned copy to trust@cyberheroeshq.com.