

QUANTCORE LEARNING HUB · COMPLIANCE PACKET

Security & Data-Privacy Compliance

QuantCore.AI · Prepared for K–12 school due-diligence and the New York City Public Schools (NYCPS) vendor-compliance process

The short version. The QuantCore Learning Hub is a financial-literacy platform built for K–12 schools. We collect the minimum data needed to teach, host on SOC 2-certified infrastructure (Supabase and Vercel), and align our practices with FERPA, COPPA, New York Education Law § 2-d, and the NIST Cybersecurity Framework. Our AEGIS AI assistant analyzes public market data only — it never sends student names, emails, IDs, grades, or any education record to an external AI service. This document records our readiness for the NYCPS vendor-compliance process and is intended to support OneTrust, DPA, IT Security Review, and OTI Cloud Review submissions.

Live, always-current versions: [Compliance](#) · [Sub-processors](#) · [Parents' Bill of Rights](#)

1. NYCPS Vendor-Compliance Process

As a web-based, AI-enabled product that handles student data, the Learning Hub is prepared to satisfy all four components of the NYCPS data-privacy and security review. The table below states each requirement and how we meet it. We are ready to begin the moment a school initiates a request, and we complete all required components concurrently.

Requirement	What We Provide	Status
OneTrust Vendor Assessment	We provide complete organization details, an accurate accounting of the student data we access and store, full AI-technology disclosures, and our IT-security and cloud-services information across all required sections of the OneTrust assessment.	Ready Responses prepared; AEGIS disclosed as an AI feature with its data flow documented (Section 5).
Data Processing Agreement (DPA)	We sign the NYCPS DPA, committing to NY Education Law § 2-d and its regulations, and supply all required attachments: Services Description; Data Privacy & Security Plan; a public Parents' Bill of Rights ; Third-Party Information Security Requirements; and a Certificate of Records Disposal.	Ready We sign the NYCPS DPA and supply all attachments, including a public Parents' Bill of Rights .
IT Security Review	We document our security controls for review against the NYC Information Security Policies, ISO 27001, and NIST standards. Our safeguards map directly to the NIST Cybersecurity Framework (Section 6).	Ready Controls map to the NIST CSF (Section 6); SOC 2 Type II in progress.
OTI Cloud Review	We complete the Cloud Review for the NYC Office of Technology & Innovation, documenting our cloud architecture and the SOC 2-certified providers (Vercel + Supabase) on which the platform runs (Sections 4 & 7).	Ready Delivered via SOC 2-certified cloud (Vercel + Supabase); architecture in Sections 4 & 7.

Our readiness commitment. Our OneTrust responses, DPA attachments, security documentation, and cloud-review materials are prepared in advance. Once a school initiates a request, we respond promptly and complete all four components concurrently so the review proceeds without delay on our side.

2. Regulatory & Standards Alignment

Framework	How We Align
FERPA (20 U.S.C. § 1232g)	When a school uses the Learning Hub we act as a “school official” with a legitimate educational interest under 34 C.F.R. § 99.31(a)(1). Education records stay under the school’s control; we are bound by FERPA’s re-disclosure limits.
NY Education Law § 2-d & Part 121	We sign the NYCPS DPA, publish a Parents’ Bill of Rights , maintain a Data Security & Privacy Plan, and meet the breach-notification and data-return obligations of § 2-d.
Chancellor’s Regulation A-820	We handle student records consistent with the confidentiality and disclosure rules of A-820.
COPPA	For students under 13 on school accounts, the school provides consent under the FTC school-authorization doctrine. We do not collect personal information from children under 13 outside the school context.
NIST Cybersecurity Framework	Safeguards organized around Identify, Protect, Detect, Respond, Recover (Section 6).
ISO 27001 / NYC Information Security Policies	Controls map to ISO 27001 domains and the NYC Information Security Policies evaluated in the IT Security Review.
State student- & consumer-privacy laws	SOPIPA (CA) and the consumer-privacy laws of CA (CCPA/CPRA), VA, CO, CT, UT and others as they take effect — strictest applicable standard applied everywhere.

3. What Data We Collect — and Minimize

We collect only what is necessary to operate a financial-literacy platform. Student data is collected on behalf of, and controlled by, the school.

Category	Examples	Purpose
Account information	Name, school email, grade level, school name (school accounts); password handled by our authentication provider.	Create and secure accounts; deliver grade-appropriate content.
Learning activity	Lessons completed, quiz/exam scores, simulated (paper) trading results, progress.	Deliver lessons, track progress, report to teachers.
AEGIS queries	The market questions a student types and the AI’s responses.	Provide market-analysis tutoring; stored as conversation history scoped to the account.
Device & technical data	IP address, browser/OS, log data, error telemetry.	Operate, secure, and debug the platform.

What we never collect: Social Security numbers, government IDs, biometric data, precise geolocation, financial-account credentials, or any data unrelated to financial-literacy education.

4. Where the Platform Runs (Cloud Infrastructure)

The Learning Hub is hosted and operated entirely within the United States on established, independently certified cloud providers. This is the basis of our OTI Cloud Review submission.

Provider	Role	Certifications / Notes
Vercel	Application hosting and global edge delivery for the web app and APIs.	SOC 2 Type II; ISO 27001; TLS in transit.
Supabase (PostgreSQL)	Primary database for accounts, learning records, and AEGIS history. US regions.	SOC 2 Type II; HIPAA-eligible; AES-256 at rest; TLS in transit; row-level security.
Upstash Redis	Caching and rate limiting.	SOC 2; encryption in transit and at rest.
Market-data & AI providers	Public market data (Polygon, Unusual Whales, CoinMarketCap) and the AEGIS language model (xAI).	Receive market data and the user's typed query only — never student records (Section 5).

A current, itemized list of sub-processors is maintained at qntcore.ai/subprocessors and updated whenever it changes. Every sub-processor is contractually bound to confidentiality, security, and use restrictions equivalent to ours.

5. The AEGIS AI Assistant — How It Handles Data

The single most important fact. AEGIS is a market-analysis tutor. It sends public market data and the market question the student types to an external language model (xAI's Grok) to generate a written analysis. It does not send student names, email addresses, student IDs, grades, school identifiers, demographic data, or any education record to that model. No personally identifiable student information leaves our infrastructure to reach the AI.

5.1 What AEGIS is for

AEGIS (“Analytical Engine for Generating Intelligent Signals”) helps students understand markets. A student asks about an asset — such as a stock, and AEGIS returns an educational, institutional-style briefing. The Learning Hub's simulated trading focuses on stocks; all trading on the platform is simulated, and AEGIS provides analysis for learning, not financial advice.

5.2 Exactly what is sent to the external AI model

When a student submits a query, our backend assembles a payload for the language model containing only:

- The market question the student typed (e.g. a ticker symbol or a sentence about a market).
- Public market data fetched from financial-data providers: prices, volume, technical indicators (RSI, MACD), market capitalization, options data (Greeks, open interest), macro snapshots (S&P 500, US Dollar Index, 10-year Treasury yield), and public news headlines for the asset.
- A fixed system instruction defining AEGIS's analytical persona and output format.
- For follow-up questions, the prior questions and AEGIS answers in that conversation, used purely as context.

That is the complete list. The payload is constructed deterministically by our code from market-data feeds — there is no field for a student's name, email, ID, grade, school, or any other identifier, and none is added.

5.3 How a student's identity is kept separate

Students must be signed in to use AEGIS, and we store each conversation so a student can revisit it. We do this using an internal account identifier (a random user ID) that lives only in our database. That identifier is used to scope and retrieve history on our servers; it is not included in the request to the external AI model. The link between a conversation and a real student exists only inside our SOC 2-certified database, never at the AI provider.

5.4 The AI provider does not train on our data

AEGIS uses xAI's Grok model through xAI's business API (api.x.ai), governed by xAI's enterprise terms — not the consumer Grok product. Under those terms, business API inputs and outputs are not used to train xAI's foundation models in the way consumer chats may be, and xAI offers a Zero Data Retention (ZDR) option for enterprise accounts under which prompts and completions are processed in real time and never persisted. Because our payload already excludes all student PII, even the data that does transit to the model contains no education record.

5.5 Transparency, bias, and human understanding

Consistent with NYCPS AI guidance, AEGIS:

- Is clearly disclosed to schools as an AI feature, with this documented data flow.
- Produces explanations a student and teacher can read and understand — a stated verdict and reasoning, not an opaque score alone.
- Does not make consequential decisions about students (no grading, discipline, or eligibility decisions). It is an educational explainer.
- Is held to the same privacy and security standards as the rest of the platform; we will notify NYCPS if we add or change AI features.
- Carries an explicit disclaimer that its output is algorithmic market analysis for educational use, not financial advice.

5.6 The data-flow, step by step

1. Student types a market question in the Learning Hub and is authenticated.
2. Our backend fetches public market data for the asset from financial-data providers.
3. A deterministic engine computes technical indicators from that market data.
4. We send the market question + market data to xAI's Grok API to write the narrative analysis. No PII is included.
5. The streamed answer is returned to the student.
6. The question and answer are saved to our database, scoped by internal user ID, so the student can revisit the conversation. The student can delete a conversation at any time.

6. How We Protect Information

Control	How We Implement It
Encryption	Personal information encrypted in transit (TLS 1.2+) and at rest (AES-256). Backups encrypted.
Access control	Authenticated sessions for all student-facing features; least-privilege access to production data; database row-level security.
Use limitation	Data used only for the contracted educational purpose. We never sell personal information, use student data for advertising, or train AI models on identifiable student data.
Breach notification	We notify affected schools, users, and regulators of any unauthorized release without unreasonable delay, applying the strictest applicable timeline (as short as 7 calendar days in some states).
Monitoring & logging	Application monitoring and error tracking (Sentry) to detect and respond to incidents.
Data return / destruction	On contract termination, student data is returned to the school or securely destroyed within 60 days, with written confirmation on request.
Independent assurance	Hosted on SOC 2 Type II-certified infrastructure; our own SOC 2 Type II assessment is in progress.

7. Sub-processors

Sub-processor	Function	Data Received
Vercel	Application hosting / edge delivery	Encrypted application traffic; log/technical data.
Supabase	Database & authentication	Account data, learning records, AEGIS history.
Upstash	Caching / rate limiting	Transient technical data.
xAI	AEGIS language model (market analysis)	Market data + the user's typed query only — no student PII.
Polygon / Unusual Whales / CoinMarketCap	Public market-data feeds	Asset symbols only; no student data.
Sentry	Error monitoring	Technical error telemetry.

8. Data Retention & Destruction

- **School-managed accounts:** governed by the school's DPA. By default, student data is returned to the school or securely destroyed within 60 days of contract termination.
- **AEGIS conversation history:** retained while the account is active; deletable by the user at any time and removed with the account.
- **Backups:** rotated out within 90 days.

After these periods, information is deleted or de-identified.

9. Compliance Contacts

For the NYCPS review, a DPA, our Data Security & Privacy Plan, or any security questionnaire, contact us at:

- **Email:** info@qntcore.ai (subject: "School Compliance" or "DPA Request")
- **Privacy requests:** info@qntcore.ai (subject: "Privacy Request")
- **School privacy contact:** designated under our DPA with each school
- **Website:** qntcore.ai & hub.qntcore.ai

We respond to all compliance and due-diligence inquiries promptly and can provide our DPA, Data Security & Privacy Plan, Parents' [Bill of Rights](#), and completed security questionnaires on request.

© 2026 QuantCore.AI. All rights reserved. This document describes our compliance posture to assist school due-diligence reviews; it is not a contract. The live version is published at qntcore.ai/compliance.