

DATA PRIVACY AND SECURITY PLAN

Prepared by Popfizz Corp. (the “Contractor”) in connection with the New York State Education Law § 2-d Rider with Harborfields Central School District (the “District”)

This Data Privacy and Security Plan (the “Plan”) describes the administrative, operational, and technical safeguards and practices that Popfizz Corp. maintains to protect Protected Data, including personally identifiable information (“PII”) from student records and from the records relating to the annual professional performance reviews of classroom teachers and principals, that the Contractor may receive under its agreement with the District. This Plan is incorporated into and attached to the Education Law § 2-d Rider and is intended to satisfy the requirements of New York Education Law § 2-d and Part 121 of the Regulations of the Commissioner of Education, including Section 121.3.

Contractor product covered by this Plan: GoCobi, the K-12 computer science and AI learning platform operated by Popfizz Corp.

1. Administrative, Operational, and Technical Safeguards

The Contractor maintains a written information security program with the following safeguards and practices in place to protect the PII it receives under the contract:

- Administrative safeguards: documented information security policies; designation of personnel responsible for data security and privacy; role-based access controls; onboarding and offboarding procedures that provision and revoke access; and periodic review of access rights.
- Operational safeguards: least-privilege access limited to employees and authorized subcontractors who need the data to provide the contracted services; logging and monitoring of access to systems that store PII; and change-management procedures for production systems.
- Technical safeguards: network and application-level access controls; multi-factor authentication for administrative access; encryption of PII in transit and at rest (see Section 8); vulnerability management and patching; and regular backups.

Hosting and infrastructure: Protected Data is stored and processed using Amazon Web Services (AWS) in the United States. AWS maintains industry-recognized security certifications for its data centers and infrastructure.

2. Compliance with Part 121 (Section 121.3)

The Contractor's practices are designed to comply with the requirements of Section 121.3 of Part 121. In particular, the Contractor:

- Limits internal access to PII to only those employees or subcontractors that need access to provide the contracted services;
- Does not use PII for any purpose not explicitly authorized in the contract;
- Does not disclose PII to any other party without the prior written consent of the parent or eligible student, except (a) to authorized representatives such as a subcontractor or assignee carrying out the contract in compliance with state and federal law, or (b) as required by statute or court order, in which case the Contractor will provide notice of disclosure to the District no later than the time the information is disclosed, unless expressly prohibited by the statute or court order;

- Maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;
- Uses encryption to protect PII in its custody while in motion and at rest; and
- Does not sell PII and does not use or disclose it for any marketing or commercial purpose, nor facilitate or permit any other party to do so.

3. Alignment with the NIST Cybersecurity Framework (Section 121.5(a))

The Contractor has adopted technologies, safeguards, and practices that align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework referenced in Part 121.5(a). The Contractor's controls map to the Framework's core functions:

- Identify: inventory of systems and data flows that involve PII, and assignment of data-protection responsibilities.
- Protect: access controls, encryption, secure configuration, and workforce training.
- Detect: logging, monitoring, and alerting for anomalous or unauthorized activity.
- Respond: a documented incident-response process (see Section 5).
- Recover: backups and restoration procedures to maintain availability and integrity of data.

4. Training on Confidentiality Laws

Officers and employees of the Contractor, and its assignees, who have access to student data or teacher or principal data receive training on the federal and state laws governing the confidentiality of such data prior to receiving access. Training covers FERPA, New York Education Law § 2-d, and Part 121, and the Contractor's internal data-handling policies. Training is refreshed on a periodic basis and upon material changes to applicable law or Contractor policy.

Training is completed prior to access and refreshed on a periodic basis, and completion is tracked and recorded by the Contractor.

5. Data Security and Privacy Incident Management

The Contractor maintains a documented process to identify, respond to, and manage data security and privacy incidents that implicate PII, including breaches and unauthorized disclosures. Upon discovery of a breach or unauthorized release of Protected Data, the Contractor will:

- Take prompt action to contain and investigate the incident;
- Notify the District without unreasonable delay and in the most expedient way possible, and in no case later than required by Education Law § 2-d and Part 121;
- Cooperate with the District and provide information reasonably necessary for the District to meet its own notification obligations; and
- Promptly reimburse the District for the full cost of notifying affected parents, eligible students, teachers, or principals where the unauthorized release is attributable to the Contractor, its subcontractors, or assignees.

Incident contact: reports and notifications may be directed to Popfizz Corp. at hello@gocobi.com.

6. Use and Management of Subcontractors

Where the Contractor engages a subcontractor, affiliate, or other entity that may receive, collect, store, record, or display Protected Data to perform its contractual obligations, the Contractor manages those relationships so that the data-protection obligations imposed on the Contractor by state and federal law and by contract flow down to and apply to the subcontractor. The Contractor uses written agreements with such parties that require equivalent safeguards, and reviews subcontractor security practices as appropriate.

Current third-party service providers used to deliver the GoCobi service include:

- Amazon Web Services (AWS) — hosting and infrastructure;
- Google — email services and authentication;
- Stripe — payment processing; and
- Anthropic — AI-assisted grading (AI Grader).

When the AI Grader feature is used, submitted student work is processed by Anthropic. The Contractor does not send student names or email addresses to Anthropic with these submissions. Additional detail on the Contractor's service providers is available at <https://gocobi.com/privacy>.

7. Data Retention, Return, and Destruction

Upon expiration, non-renewal, or termination of the agreement, the Contractor will, at the District's option and direction, return all of the District's data (including all Protected Data) in its possession by secure transmission, transition it to a successor contractor, or delete or destroy it. Where deletion or destruction is directed, the Contractor will use methods designed to render the data unrecoverable and will confirm completion to the District upon request.

Retention during the term: Protected Data is retained only for as long as reasonably necessary to provide the contracted educational services, maintain educational records requested by the District, and fulfill contractual or legal obligations. Student information may remain in the Contractor's systems after the District stops using the service until the District requests deletion or the information is no longer reasonably necessary for the purposes for which it was collected. The Contractor's retention policy is available at <https://gocobi.com/privacy>.

8. Encryption

The Contractor uses encryption to protect PII in its custody both in motion and at rest. Data in transit is protected using industry-standard transport-layer encryption (HTTPS/TLS), and data at rest is protected using industry-standard encryption provided through its AWS infrastructure. The Contractor's encryption practices are intended to meet or exceed the standard required by the Secretary of the U.S. Department of Health and Human Services under HIPAA, consistent with Education Law § 2-d.

9. Use Limitations; No Sale or Commercial Use

The Contractor uses Protected Data only for the purposes explicitly authorized in the agreement. The Contractor does not sell Protected Data and does not use or disclose it for any marketing or commercial purpose, nor facilitate or permit any other party to do so. Where a parent or eligible student requests a service or product from the Contractor and provides express consent to the use or disclosure of PII for purposes of providing the requested product or service, such use is not treated as a prohibited marketing or commercial purpose.

10. Parents' Bill of Rights

The Contractor acknowledges and will comply with the District's Parents' Bill of Rights for Data Privacy and Security. The Contractor's execution of the Education Law § 2-d Rider constitutes its acknowledgement, acceptance, and signature of the District's Parents' Bill of Rights.

Contractor Contact for Data Privacy and Security

Company: Popfizz Corp. • Product: GoCobi

Address: 690 Saratoga Ave. STE 100, San Jose, CA 95129, United States

Data Privacy Contact: Popfizz Corp. Privacy Team

Email: hello@gocobi.com

Privacy Policy: <https://gocobi.com/privacy>