EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Popfizz Corp. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Harborfields Central School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

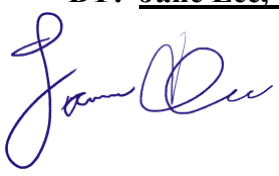
In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER: Popfizz Corp.

BY: Jane Lee, CEO **DATED: 9/19/2025**



DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Popfizz Corp.

Data Privacy and Security Plan

This Data Privacy and Security Plan ("Plan") is adopted by Popfizz Corp. (the "Contractor") in compliance with New York State Education Law § 2-d, Part 121 of the Commissioner's Regulations, FERPA, CIPA, HIPAA (as applicable), and the requirements of the Harborfields Central School District (the "District"). This Plan describes the safeguards, policies, and practices used to protect Protected Data entrusted to Popfizz Corp.

---

1. Safeguards to Protect Data

Popfizz Corp. maintains administrative, technical, and physical safeguards aligned with the **NIST Cybersecurity Framework** to ensure the confidentiality, integrity, and availability of Protected Data. Measures include strong authentication protocols, encryption of data in transit and at rest, access logging, and periodic security reviews.

2. Compliance

Popfizz Corp. complies with all applicable laws and regulations, including **Education Law § 2-d**, **FERPA**, **CIPA**, **HIPAA** (if applicable), and **Part 121** of the Commissioner's Regulations, as well as the District's data security and privacy policy.

3. Employee Training

All employees with access to Protected Data receive training on federal and state confidentiality laws, including FERPA and Education Law § 2-d, prior to being granted access. Refresher training is conducted annually or as needed when laws or regulations change.

4. Subcontractor Management

If Popfizz Corp. engages subcontractors, each subcontractor must agree in writing to comply with the same data protection obligations set forth by law and in this Plan. Subcontractor contracts include provisions requiring adherence to encryption, access restrictions, and breach response protocols.

5. Incident Response and Breach Notification

Popfizz Corp. maintains an incident response process to identify, contain, investigate, and remediate data security incidents. In the event of a breach or unauthorized disclosure of Protected Data, Popfizz Corp. will:

- Notify the District promptly, within **[insert number, e.g., 24 or 48] hours** of discovery.
- Provide details of the incident, data affected, and corrective measures taken.
- Fully cooperate with the District in notifying affected individuals and mitigating harm.

6. Data Return or Destruction

Upon contract expiration, termination, or at the District's direction, Popfizz Corp. will securely return all Protected Data to the District or permanently delete/destroy such data. Secure deletion methods include cryptographic erasure or secure wipe processes consistent with industry standards.

7. Encryption and Storage

All Protected Data is encrypted **in transit (TLS 1.2 or higher)** and **at rest (AES-256 or equivalent)**. Data is stored only on secure systems protected by firewalls, intrusion detection, and continuous monitoring.

8. Prohibition on Sale or Marketing Use

Popfizz Corp. does not sell Protected Data, nor does it use or disclose Protected Data for marketing or commercial purposes. Data is used solely to provide contracted services to the District.