ADDENDUM TO AGREEMENT
Regarding
Data Privacy and Security
In Accordance with Section 2-d of the New York Education Law

This is an addendum (the "Addendum") to an agreement entered into by between **_KEV Group Inc_**, with its principal place of business located at **3000 S Hulen St, Fort Worth, TX 76109, USA** ("Contractor"), and the **Wappingers Central School District**, with its principal place of business located at 25 Corporate Park Drive Hopewell Junction NY, 12533 (**"District"**). Upon being executed by Contractor's and District's authorized representatives, this Addendum shall be deemed to have been in full force and effect as of the effective date of the Agreement it amends.

WHEREAS, the District is an educational agency within the meaning of New York State Education Law, Section 2-d ("Section 2-d"), and Contractor is a third-party contractor within the meaning of Section 2-d; and

WHEREAS, Contractor and its authorized officers, employees, students and agents shall have access to "student personally identifiable information (PII)," "student data" and/or "teacher or principal data" regulated by Section 2-d; and

WHEREAS, the provisions of this Addendum are intended to comply with Section 2-d in all respects. To the extent that any term of the Agreement conflicts with the terms of this Addendum, the terms of this Addendum shall apply and be given effect.

NOW, THEREFORE, it is mutually agreed that the Agreement is hereby amended in accordance with this Addendum, as follows:

1.   **Confidential Information**

1.1   Contractor agrees that in performing the Original Agreement with the District, Contractor may have access to confidential information in the possession of the District, including student, teacher or principal personally identifiable information ("PII"). For the purposes of this Addendum and the Original Agreement, it is agreed that the definition of Confidential Information includes all documentary, electronic or oral information made known to Contractor or developed or maintained by Contractor through any activity related to the Original Agreement. This Confidential information includes student, teacher and/or principal data (as the terms are defined under Section 2-d.

1.2   Contractor agrees to comply with Section 2-d, and the corresponding regulations promulgated by the Commissioner of Education of New York ("Commissioner") thereunder. In addition, Contractor agrees to comply with any changes in Section 2-d, or the Commissioner's regulations that may be amended or modified during the term of the Original Agreement. Upon request by the District, Contractor shall provide the District with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not

violate Contractor's own information security policies, confidentiality obligations, and applicable laws.

1.3 Upon expiration of the Agreement to which this Addendum applies, without a successor agreement in place, Contractor shall assist the District in exporting all student, teacher and/or principal data previously received by Contractor from, or developed on behalf of, the District, and Contractor shall, at the request of the District, either securely delete any student, teacher and/or principal data remaining in Contractor's possession or return the student, teacher and/or principal data to the District. If student, teacher and/or principal data is to be maintained by Contractor for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Contractor in a secure data facility located within the United States.

1.4 The parties further agree that the terms and conditions set forth in this Confidential Information section and all of its subparts shall survive the expiration and/or termination of the Original Agreement.

2. Data Inspection and Challenges to Data

Education Law Section 2-d and FERPA provide parents and eligible students the right to inspect and review their child's or the eligible student's PII stored or maintained by the District. To the extent PII is held by Contractor pursuant to the Original Agreement, Contractor shall respond within thirty (30) calendar days to the District's requests for access to PII so the District can facilitate such review by a parent or eligible student. If a parent or eligible student contacts Contractor directly to review any of the PII held by Contractor pursuant to the Original Agreement, Contractor shall promptly notify the District and refer the parent or eligible student to the District.

In the event that a student's parent or an eligible student wishes to challenge the accuracy of student data (pertaining to the particular student) that may include records maintained, stored, transmitted, and/or generated by Contractor pursuant to the Agreement, the challenge will be processed in accordance with the procedures of the District.

A teacher or principal who wishes to challenge the accuracy of data pertaining to the teacher or principal personally, which is disclosed to Contractor pursuant to the Agreement, shall do so in accordance with the procedures for challenging APPR data, as established by the District.

3. Training

Contractor represents and warrants that any of its officers, employees, and/or assignees who will have access to student, teacher and/or principal data pursuant to the Original Agreement will receive training on the federal and state laws governing confidentiality of such student, teacher and/or principal data, prior to obtaining initial or any further access to such data.

4. Use/Disclosure of Data

4.1   Contractor shall not sell or use for any commercial purpose student, teacher and/or principal data that is received by Contractor pursuant to the Agreement or developed by Contractor to fulfill its responsibilities pursuant to the Agreement.

4.2   Contractor shall use the student, teacher and/or principal data, records, or information solely for the exclusive purpose of and limited to that necessary for the Contractor to perform the duties and services required under the Original Agreement. Such services include, but are not limited to please **refer to signed SOW**. Contractor shall not collect or use educational records of the District or any student, teacher and/or principal data of the District for any purpose other than as explicitly authorized in this Addendum or the Original Agreement.

4.3   Contractor shall ensure, to the extent that it receives student, teacher and/or principal data pursuant to the Agreement, that it will not share Confidential Information with any additional parties, including an authorized subcontractor or non-employee agent, without prior written consent of the District. Contractor shall indemnify and hold the District harmless from the acts and omissions of the Contractor's employees and subcontractors.

5.   Contractor's Additional Obligations under Section 2-d and this Addendum

Contractor acknowledges that, with respect to any student, teacher and/or principal data received through its relationship with the District pursuant to the Agreement it is obliged to maintain a Data Security & Privacy Plan, and fulfill the following obligations:

- execute, comply with and incorporate to this Addendum as Exhibit A, as required Section 2-d, the Parents' Bill of Rights for Data Privacy and Security developed by the District, as well as the supplemental information in Exhibit B;
- store all data transferred to Contractor pursuant to the Agreement by the District, in an electronic format on systems maintained by Contractor in a secure data facility located within the United States or hard copies under lock and key;
- limit internal access to student, teacher and/or principal data to Contractor's officers, employees and agents who are determined to need such access to such records or data to perform the services set forth in the Original Agreement;
- not disclose student, teacher and/or principal data to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under the Agreement, unless: (I) the other party has the prior written consent of the applicable student's parent or of the eligible student; or (II) the other party has the prior written consent of the applicable teacher or principal; or (III) the disclosure is required by statute or court order, and notice of the disclosure is provided to the District no later than five business days before such information is required or disclosed (unless such notice is expressly prohibited by the statute or court order);
- use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to encryption, firewalls and password protection as

4

specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5, Section 13402(H)(2), to protect the security, confidentiality and integrity of student and/or staff data of the District while in motion or in custody of Contractor from unauthorized disclosure;

- not mine Confidential Information for any purposes other than those agreed to in writing by the Parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited; notify the District, in the most expedient way possible and without unreasonable delay, of any breach of security resulting in an unauthorized release of any PII. In addition, Contractor shall take immediate steps to limit and mitigate the damage of such security breach or unauthorized release to the greatest extent practicable, and promptly reimburse the District for the full cost of any notifications the District makes as a result of the security breach or unauthorized release. Contractor further acknowledges and understands that Contractor may be subject to civil and criminal penalties in accordance with Section 2-d for violations of Section 2-d and/or this Agreement.

- understand that any breach of the privacy or confidentiality obligations set forth in this Addendum may, at the sole discretion of the District, result in the District immediately terminating this Agreement; and

- familiarize its applicable officers, employees and agents with this Addendum and with the "Parents' Bill of Rights for Data Privacy and Security."

The Contractor acknowledges that failure to fulfill these obligations shall be a breach of the Agreement.

6.   Except as specifically amended herein, all of the terms contained in the Original Agreement are hereby ratified and confirmed in all respects, and shall continue to apply with full force and effect.

IN WITNESS WHEREOF, Contractor and the District execute this Addendum to the Agreement as follows:

Contractor   District

                                                              Daren Lolkema
By: **Joshua Shuval**   By: _____~~Assistant Superintendent~~_

Title: Director of Operations & Risk Management   Title: _____

Signature: [Signed by: B5E99DC24F4D45A...]   Signature: _____

Date: 3/12/2025   Date: 3 / 12 / 25

Exhibit A

District's Parents' Bill of Rights

http://go.boarddocs.com/ny/wcsd/Board.nsf/goto?open&id=BPZGZJ463DB1

PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT

The ____**KEV Group Inc_** has been engaged by the Wappingers Central School District to provide services. In this capacity, the company may collect, process, manage, store or analyze student or teacher/principal personally identifiable information (PII).

The __**KEV Group Inc___** will provide the district with (*describe specific purpose for which the PII will be used*)

SchoolCash integrates with the district's Student Information System (SIS) via API or Secure File Transfer to receive student data, including first name, last name, school, grade, homeroom, courses, guardian name, and email. This enables fees to be assigned based on these criteria, allowing parents/guardians to receive notifications about their child's fees and school staff to track payments efficiently. The collected data is used exclusively for managing and collecting Student Activity Fees.

The **_KEV Group Inc_** will ensure that subcontractors or others that the company shares PII will abide by data protection and security requirements of district policy, and state and federal law and regulations by (*describe methods/procedures to safeguard data use by subcontractors*).

PII will be stored (*describe the location in a manner that protects data security*)

- **No subcontractor access** – KEV Group Inc. does not grant subcontractors access to PII.
- **Secure storage** – All PII data is stored in **Azure US** and is **encrypted at rest and in transit**.
- **Backup security** – Backups are also stored in **Azure US** to maintain data security.
- **Access control** – Database access is managed through **Role-Based Access Control (RBAC)**.
- **Regular reviews – Access permissions are reviewed quarterly** to ensure compliance with security policies.

Parents may challenge the accuracy of PII held by **this vendor** by contacting the Wappingers CSD Office of Compliance and Information Systems at 25 Corporate Park Drive Hopewell Junction NY, 12533 (or by phone 845-298-5000 Ext 40131, or by email: daren.lolkema@wcsdny.org).

The **_KEV Group Inc_** will take reasonable measures to ensure the confidentiality of PII by implementing the following (*describe the following, as applicable*):

- **Password protections :** Enforces strong password policies, including complexity requirements, expiration policies, and multi-factor authentication (MFA) where applicable.
- **Administrative procedures :** Implements access controls based on the principle of least privilege, conducts regular security training, and performs quarterly access reviews.
- **Encryption :** Ensures PII is **encrypted both in transit and at rest** using industry-standard encryption protocols.

- **Firewalls** : Deploys Web Application Firewalls to protect from various online threats, such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Distributed Denial-of-Service (DDoS) attacks, Zero-day exploits, Bot attacks

The contractor's agreement with the district begins on **_March 1, 2025_____** and ends on **_ June 30, 2026 (Renewable)_____**. Once the contractor has completed its service to the district, records containing student PII will be **(select one: destroyed or returned): _____Destroyed____** by dropping/deleting the database

When a district is no longer a customer, the assigned Customer Service Manager submits a ticket for decommissioning. The DevOps team deletes the configuration and databases, and backups are automatically deleted after the 10-business-day retention period.

Exhibit B

Supplemental Information

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	KEV Group Inc
Description of the purpose(s) for which Contractor will receive/access PII	SchoolCash integrates with the district's Student Information System (SIS) via API or Secure File Transfer to receive student data, including first name, last name, school, grade, homeroom, courses, guardian name, and email. This enables fees to be assigned based on these criteria, allowing parents/guardians to receive notifications about their child's fees and school staff to track payments efficiently. The collected data is used exclusively for managing and collecting Student Activity Fees.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date _____ **March 1, 2025**_____ Contract End Date ____ **June 30, 2026 (Renewable)**____

Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☒ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
	Signed by:
[Signature]	B5E00DC24F4D46A...

[Printed Name]	Joshua Shuval
[Title]	Director of Operations and Risk Management
Date:	March 10, 2025