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 "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 Valley Stream UFSD 30 (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. 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 Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), 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 New York State ("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.

2. 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.

Contractor's Data Security and Privacy Plan Requirements

3. 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:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify 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;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify 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 District;
g. Describe whether, how and when 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 Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or subcontractors that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or

ii. 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.

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

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

h. 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.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be used;

b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;

d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

e. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data,

Contractor shall immediately notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

Superintendent of Schools
Valley Stream UFSD 30
175 N. Central Avenue, Suite 220
Valley Stream, NY 11580

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars ($10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.

10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event a Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from 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: Wallwisher, Inc. (d/b/a Padlet)

Signature: Zoheb Jamal **Date:** 4 November 2025

Printed Name: Zoheb Jamal **Title:** VP of Growth

EXHIBIT "A"

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. This document contains a plain-English summary of such rights.

- A student's personally identifiable information cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Valley Stream Union Free School District Thirty.
- State and Federal Laws protect the confidentiality of personally identifiable student information, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred.
- A complete list of all student data elements collected by New York State is available for review at the following website: http://www.p12.nysed.gov/irs/sirs

The list may also be made available by writing to:

Office of Information & Reporting Services
New York State Education Department
Room 863 EBA,
89 Washington Avenue
Albany, NY 12234

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Valley Stream UFSD 30
Attn: Data Protection Officer
175 N. Central Avenue, Suite 220
Valley Stream, New York 11580
Marcela Moran
516-434-3642

OR

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234
Email: CPO@mail.nysed.gov

- Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

    - The exclusive purposes for which the student data or teacher or principal data will be used.
    - How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
    - When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.
    - If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
    - Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

- Third-party contractors are also required to:

    - Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
    - Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
    - Not use educational records for any other purpose than those explicitly authorized in the contract;
    - Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
    - Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
    - Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
    - Notify the District of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
    - Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
    - Provide a signed copy of this Bill of Rights to the District thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

- This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Contractor: Wallwisher, Inc. (d/b/a Padlet)

Signature: Zoheb Jamal **Date:** 4 November 2025

Printed Name: Zoheb Jamal **Title:** VP of Growth

EXHIBIT "B"
Contractor's Supplemental Information

Name of Contractor	Wallwisher, Inc. (d/b/a Padlet)
Description of the purpose(s) for which Contractor will receive/access PII	Provide and optimise delivery of the Padlet platform to the users including maintenance of institutional accounts, storage, hosting of content uploaded by users, providing access to content for cohorts of users; maintaining access controls and the privacy status of content and application of records retention and destruction policies in accordance with the LEA's instruction; and aggregate and anonymize Student Data ("de-identify") in accordance with applicable law and use such resulting data set for its purposes.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Agreement Term	Agreement Start Date: 31 July 2025 Agreement End Date: 31 July 2026
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement 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 Agreement. (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 District, or a successor contractor at the District'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 District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District'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: Wallwisher, Inc. (d/b/a Padlet)

Signature: Zoheb Jamal **Date:** 4 November 2025

Printed Name: Zoheb Jamal **Title:** VP of Growth

EXHIBIT "C"
Contractor's Data Security & Privacy Plan

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

PADLET DATA SECURITY AND PRIVACY PLAN

Wallwisher Inc. (d/b/a Padlet) (hereinafter the “Provider”, “We”, “our” or “us”) and ___________________________ (hereinafter referred to as “LEA”, “Customer”) hereby agree to make this Data Security and Privacy Plan part of their Agreement, dated _______________ __, 20__, for products and services pursuant to the Service Agreement.

1. Definitions: Terms used in this Data and Security Privacy Plan (hereinafter the “Plan”) shall have the same meanings as those found in Education Law Section 2-d(1) and the Regulations of the Commissioner of Education at Section 121.1 of Title 8 of the New York Codes, Rules and Regulations (8 NYCRR § 121.1)

2. Outline how the Provider will implement all state, federal and local data security and privacy requirements over the term of the Agreement in a manner that is consistent with the data security and privacy policies of LEA that purchase Provider’s products and/or services pursuant to the Agreement.

Padlet implements all state, federal and local security and privacy requirements by:

(a) implementing encryption of data 'at rest' with AES 256 bit encryption and while in transit with at least TLS 1.2 encryption

(b) tracking and logging of personnel interactions with School District data,

(c) limiting the access to Padlet systems to authorized users only

(d) updating the systems as new requirements are promulgated.

(e) providing data privacy and security training for all employees who have access to School District data

(f) conducting criminal background checks on all employees where the laws permit

(g) requiring that all employees and contractors execute confidentiality agreements to protect School District data

(h) committing to use personal data in line with terms of the DPA.

3. Specify the administrative, operational and technical safeguards and practices the Provider has in place to protect personally identifiable information that it receives, maintains, stores, transmits or generates pursuant to the Agreement.

The security of your personal information is important to us. We maintain administrative, technical and physical safeguards to protect against loss, theft, unauthorized use, disclosure, or retrieval of personal information. In particular:

- We perform application security testing; penetration testing; conduct risk assessments; and monitor compliance with security policies
- We periodically review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems
- We continually develop and implement features to keep your personal information safe
- When you enter any information anywhere on the Service, we encrypt the transmission of that information using secure socket layer technology (SSL/TLS) by default
- We ensure passwords are stored and transferred securely using encryption and salted hashing
- The Service is hosted on servers at a third-party facility, with whom we have a contract providing for enhanced security measures. For example, personal information is stored on a server equipped with industry standard firewalls. In addition, the hosting facility provides a 24x7 security system, video surveillance, intrusion detection systems and locked cage areas
- We operate a ‘bug bounty’ security program to encourage an active community of third-party security researchers to report any security bugs to us
- We restrict access to personal information to authorized Padlet employees, agents or independent contractors who need to know that information in order to process it for us, and who are subject to strict confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.
- We require sub-processors to comply with security requirements via separate data processing agreements
- We use a Password Manager to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. We require 2FA authentication to be enabled for all services where applicable.

4. Describe how officers and employees of the Provider and its subcontractors and assignees who will have access to the student, teacher or principal data of the Customers have received or will receive training on the federal and state laws governing the confidentiality of such data prior to receiving access to the data.

   We provide periodic security training to employees and others who operate or have access to the system. The training includes text and video tutorials on the applicable data protection laws including but not limited to FERPA, COPPA, GDPR. The employees are also asked to take a quiz to confirm their understanding.

5. Will the Provider utilize sub-contractors in the performance of the Agreement?

   Yes

If Yes, how will the Provider manage the sub-contractors to ensure personally identifiable data and information is protected?

We enter into written agreements whereby Sub-processors agree to secure and protect Student Data in a manner consistent with the terms of the Agreement. We periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with the Agreement and may discipline or terminate them if they fail to meet these obligations.

6. How will the Provider manage data privacy and security incidents that involve personally identifiable data or information?

   In the event that Personally Identifiable Data is accessed or obtained by an unauthorized individual, we shall provide notification to LEA within a reasonable amount of time of the incident.

   a. We shall provide the following information:

   i. The name and contact information of the reporting LEA subject to this section.

   ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

   iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

   iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

   v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

   b. At LEA's discretion, the security breach notification may also include any of the following:

   i. Information about what the LEA has done to protect individuals whose information has been breached.

   ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

   c. As a result of a breach of the security system, we shall assist LEA with any official notifications required by State agencies.

d. At the request and with the assistance of the District, we shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.