GARDEN CITY UNION FREE SCHOOL DISTRICT
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 Wallwisher, Inc. (d/b/a Padlet) (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 GARDEN CITY UNION FREE 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: Wallwisher, Inc. (d/b/a Padlet)

BY: Zoheb Jamal **DATED:** 14 May 2025

Return to:

Lauren Maguire
Director of Information Technology
Garden City Union Free School District
56 Cathedral Avenue
Garden City, NY 11530
maguirel@gcufsd.net

DATA PRIVACY AND SECURITY 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.