DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Liverpool Central School District (hereinafter "School District") and Wallwisher, Inc (d/b/a Padlet) (hereinafter "Contractor") entered into an agreement dated 04/15/2024 (hereinafter "Agreement") for Padlet (hereinafter "Services").

WHEREAS, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s

See Exhibit A

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

See Exhibit A

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.

a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.

b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.

c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement.

d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.

e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided:
Specify date of each training

See Exhibit A

5. Subcontractors (select one): b. Contractor shall utilize subcontractors

a. Contractor shall not utilize subcontractors.

b. Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

See Exhibit A

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information:
Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.

See Exhibit A

7. Termination of Agreement.

a. Within 60 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. [x] Within 60 days of termination of the Agreement, Contractor shall Return all data to the School District using exported files ; OR

☐ Transition all data to a successor contractor designated by the School District in writing using_____.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of 04/15/2024.

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

Title: VP of Growth

Date: 04/15/2024

Parents Bill of Rights
Liverpool Central School District

The Liverpool School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, parents and eligible students can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, 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.

4. A complete list of all student data elements collected by NYSED is available for public review and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Liverpool School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

4. 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;

5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

6. Address how the data will be protected using encryption while in motion and at rest.

Daniel P Farsaci
Liverpool Administrator Signature

Daniel Farsaci
Liverpool Administrator Printed Name

04/16/2024
Date

Zoheb Jamal
Representative Signature

Zoheb Jamal
Representative Printed Name

04/15/2024
Date

EXHIBIT "A"

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.