LIBERTY CENTRAL SCHOOL DISTRICT
DISTRICT OFFICE
Stacy Feasel
District Data Coordinator and Privacy Officer
District Office, 115 Buckley St. Liberty, NY 12754
845-292-5400 x 2332

Data Processing Addendum

This Data Processing Addendum Addendum ("***Addendum***") is entered into by the Liberty Central School District (the "***District***") and Wonder Workshop Inc. ("***Contractor***") as of 7/1/24 (the "***Effective Date***").

WHEREAS, the District is committed to protecting the security and privacy of personally identifiable information ("***PII***") in accordance with all applicable state and federal laws, including but not limited to the Family Educational Rights and Privacy Act ("***FERPA***") and New York State Education Law § 2-d; and

WHEREAS, Contractor has entered into an agreement (the "***Underlying Agreement***" with the District pursuant to which the Contractor may receive PII, including PII of students, teachers and/or principals;

NOW, THEREFORE, the Parties agree as follows:

1. Definitions. All capitalized terms not otherwise defined herein shall have the same definition as used in New York State Education Law § 2-d and/or 8 NYCRR Part 121.

2. Parents Bill of Rights. The District's Parents' Bill of Rights for Data Privacy and Security ("***Parents Bill of Rights***") is attached as Exhibit A and shall be deemed to be expressly appended to and included with the Underlying Agreement.

3. Contractor Responsibilities:
   a. Contractor agrees that PII, including Student Data and Teacher or Principal Data, shall be maintained confidentially and in accordance with federal and state law and the District's data security and privacy policies.

   b. Contractor may not sell, use or disclose PII for any marketing or commercial purpose or permit another person to do so.

   c. Supplemental information concerning Contractor's handling of Student Data and/ or Teacher or Principal Data is set forth as Exhibit A-1 to the Parents Bill of Rights.

d. Contractor shall maintain a data security and privacy plan that complies with the District's data security and privacy policies, as well as all legal requirements, including but not limited to the specific requirements set forth in NY Education Law §2-d, 8 NYCRR Part 121, and the National Institute of Standards and Technology ("***NIST***") Cybersecurity Framework. At a minimum, Contractor shall:

i. limit access to PII to only those employees or subcontractors that need access to perform Contractor's obligations under the Underlying Agreement;

ii. not use PII for any purpose not authorized under the Underlying Agreement;

iii. not disclose PII to any person without the prior written consent of the parent or Eligible Student, except to the extent such disclosure is made:

1. to an authorized subcontractor for a purpose necessary to fulfill the Contractor's obligations under the Underlying Agreement; or

2. as required under applicable law;

iv. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII received pursuant to the Underlying Agreement; and

v. use encryption to protect PII while in motion or at rest.

e. If Contractor uses a third party to perform any of Contractor's obligations under the Underlying Agreement, Contractor shall ensure that the third party complies with all obligations of the Contractor under this Section 3.

4. Breach Notification. Unless otherwise expressly required by law, Contractor agrees to:

a. notify the District promptly, but in no event later than twenty-four (24) hours, after discovery of any data breach or other security incident (collectively, a "***Security Incident***") that is reasonably believed to affect the confidentiality, integrity and/or security of PII, including but not limited to the unauthorized access to or disclosure of such PII;

b. provide the District promptly, but in no event later than five (5) business days, after the notice described in Section 4(a) with a report concerning the known or suspected cause of the Security Incident, the information affected, the steps taken by the Contractor to stop and/or mitigate the Security Incident, and any

other information reasonably requested by the District or law enforcement authorities to respond to and/or otherwise recover from the Security Incident; and

c. comply with all other applicable breach notification requirements, including but not limited to those in NY Education Law § 2-d(6) and 8 NYCRR § 121.10.

5. Changes in Applicable Law. PII, including Student Data and Teacher or Principal Data, is subject to rapidly changing laws and regulations. Contractor agrees to work in good faith to execute and implement any additional documents, policies and/or procedures reasonably necessary to comply with any change in applicable law or regulation within thirty (30) days of a request by the District.

6. Termination of Underlying Agreement. Notwithstanding any other provision of the Underlying Agreement, the District may terminate the Underlying Agreement without penalty if (a) Contractor fails and/or refuses to comply with its obligations under this Addendum or (b) the parties are unable to reach agreement on an amendment to this Addendum required by changes in applicable law. At the District's written request, whether upon termination or at any other time, Contractor shall return, de-identify and/or delete all PII in its possession, custody or control. Notwithstanding the foregoing, Contractor shall be entitled to retain (a) archive copies required to be retained (i) by law, (ii) as part of Contractor's business record-keeping (such as without limitation for dispute resolution such as to establish or defend against claims) or (iii) for compliance purposes (such as without limitation audit, tax, privacy or other compliance requirements) or (b) back-up or log files that are not accessible in the ordinary course and deleted on a standard schedule (other than ad hoc back-ups that are deleted outside standard retention windows).

7. Interpretation. In the event of a conflict between the terms of this Addendum (including the attached Parents Bill of Rights) and the Underlying Agreement, the terms of this Addendum and the Parents Bill of Rights shall control notwithstanding any language in the Underlying Agreement to the contrary.

8. Counterparts. This Addendum may be executed in counterparts, each of which shall be deemed an original. Each counterpart may be executed and/or exchanged by electronic means.

IN WITNESS WHEREOF, the Parties agree to be bound by the terms of this Addendum as of the Effective Date:

Liberty Central School District:

By: Stacy Feasel

Signature:

Title: District Privacy Officer

Date: 7/1/24

Contractor:

By: Jenn Homme

Signature: Jenn Homme

Title: VP Operations

Date: June 17, 2024

Exhibit A

Liberty Central School District

Parents Bill of Rights for Data Privacy and Security

The Liberty Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Liberty Central District establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- The district and its schools, and third-party contractors and subcontractors, will not sell student PII or use or disclose it for any marketing or commercial purposes or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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 the State Education Department is available for public review at http://nysed.gov/data-privacy-security/student-data-inventory or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the District Security and Privacy Officer, at 845-292-5400 by mail to 115 Buckley Street, Liberty NY 12754 or by email to dataprivacy@libertyk12.org. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy security/report-improper-disclosure, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- All district and school employees and officers with access to PII will receive annual training on applicable federal and state laws, regulations,

district and school policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

- In the event that the district engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting (Complaints should be directed to the District Security and Privacy Officer at 845-292-5400 by mail to 115 Buckley Street, Liberty NY 12754 or by email to tdefrank@libertyk12.org or can access the information on the district's website www.libertyk12.org

Exhibit A-1

Liberty Central School District

Supplemental Information Relating to Underlying Agreement

Pursuant to New York Education Law §2-d(c) and 8 NYCRR § 121.3(c), the following additional information is provided with respect to processing of Student Data and/or Teacher or Principal Data for the Underlying Agreement between the District and Contractor:

(1) The exclusive purposes for which the Student Data or Teacher or Principal Data will be used are **described here**: **Student data used to identify users, assign curriculum and track results**

(2) Contractor will ensure that the subcontractors, persons or entities that Contractor will share the Student Data or Teacher or Principal Data with, if any, will abide by data protection and security requirements by **methods described here:** **Wonder Workshop does not utilize subcontractors**

(3) The Underlying Agreement expires as set forth in the applicable ordering document. Upon expiration of the Underlying Agreement, and upon written request from the District, Student Data, Teacher or Principal Data will be deleted, and a certification of deletion will be provided to the District.

(4) A parent, eligible student, teacher or principal may challenge the accuracy of the Student Data or Teacher or Principal Data that is collected by contacting the District's Data Protection Officer.

(5) Student Data or Teacher or Principal Data will be stored **at the location described here**: **We do not maintain our own physical environment. Cloud provider maintains high level of physical security. Backups are encrypted. User data is only available in secured databases on the cloud. Test environments do not use production user data. Test environments use the same security controls as the production environment, with separate security keys. Solution allows SSO with Google, but no data sharing.**

(6) Contractor will use the security protections **described here:** **Data in transit encrypted via TLS. Data storage and backups encrypted with AES 256. Only employees that require access to customer data have database accounts. Only high level employees have access to system administrator access. Secure operating systems, 2FA access, monitoring and logging, alarms on atypical activity and errors**

(7) Data will be protected using encryption while in motion and at rest. **Data in transit encrypted via TLS. Data storage and backups encrypted with AES 256.**