



DATA PRIVACY ADDENDUM
Confidentiality and Non-Disclosure Requirements

This Data Privacy Addendum (“DPA”) dated _____ (“Agreement”) is between Thompson School District R2-J (“District”) and _____ (“Vendor”). This DPA modifies and is incorporated into the Agreement. Notwithstanding any provision of the Agreement to the contrary, the terms of this DPA supersede all contrary or conflicting terms of the Agreement.

PRIVACY RECITALS

- A. District wishes to disclose certain information to Vendor pursuant to the work being performed by Vendor, some of which information may constitute Personally Identifiable Information (defined below).
- B. District and Vendor intend to protect the privacy and provide for the security of Personally Identifiable Information disclosed to, or collected by, Vendor pursuant to this Agreement. Vendor shall adhere to the Children’s Online Privacy Protection Rule (COPPA), 22-16-101 *et al.*, C.R.S.; the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99; and the Colorado Student Data Transparency and Security Act, HB16-1423
- C. For this DPA the Parties agree to the following Definitions:
 - a. "PII Data" means all Personally Identifiable Information (PII)
 - b. "Destroy" means to remove to best industry standards Personally Identifiable Information (“PII”) from Vendor’s systems, paper files, records, databases, and any other media regardless of format, so that it is permanently irretrievable in the Vendor’s and Subcontractor’s normal course of business. Proof of destruction via signed documentation may be required.
 - c. “Incident” means an event that results in or constitutes the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a computer or network containing PII Data disclosed by the District to the Vendor or collected from District staff/students by the Vendor pursuant to the terms of the Agreement regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a District System for the processing or storage of PII Data; (iv) a material breach of the Agreement that involves the misuse or unauthorized release of PII Data.
 - d. "Personally Identifiable Information" or “PII” means information that, alone or in combination, personally identifies an individual, or family, and that is collected, maintained, generated, or inferred by a public education entity. PII Data also includes other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
 - e. “Subcontractor” means any third party engaged by Contractor receiving or processing PII Data.
 - f. “Targeted Advertising” means selecting and sending advertisements to a student/individual based on information obtained or inferred over time from the student’s online behavior, use of applications, or PII Data.

D. General Provisions



Vendor shall comply with all laws and regulations concerning confidentiality of PII Data. Vendor shall promptly forward to the District's representative any request or demand from a third party for PII Data in the possession of Vendor. Vendor agrees that auditors so designate by the District shall have the option to audit Vendor's services, including District Systems and policies, procedures or logs related to the performance of services under the Agreement. Vendor shall send the District a written notice, which includes a clear explanation of the proposed changes prior to making a material change to Vendor's privacy policies.¹

E. Subcontractors

a. Vendor shall not use a Subcontractor or disclose PII Data to a Subcontractor unless and until the Vendor contractually requires the Subcontractor to comply with C.R.S. §§22-16-108 through 22-16-110 and the requirements of this DPA.

b. If Vendor discovers that Subcontractor or any subsequent subcontractor has committed a material breach of the contract between Vendor and Subcontractor that involves the misuse or unauthorized release of PII Data, Vendor acknowledges that the District may terminate the contract with Vendor unless Vendor terminates the contract with Subcontractor as soon as possible after Vendor knows or has reason to know of Subcontractors' or any subsequent subcontractors' material breach.

F. End of Agreement

a. Upon request by the District made before or within thirty (30) calendar days after termination of the Agreement, Vendor shall make available to the District a complete and secure (i.e. encrypted and appropriately authenticated) download file of all data, including, but not limited to, all PII Data, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format.

b. Following the termination of this Agreement plus thirty (30) calendar days, Vendor shall destroy all PII Data collected or generated as a result of this Agreement within the following thirty (30) days after the request period in provision D.1 above. The Vendor shall notify and attest to the District of the date upon which all of the PII Data is destroyed via a signed document.

G. Use

a. During the term of this Agreement, if the District requests the destruction of PII Data collected, generated or inferred as a result of this Agreement, the Vendor shall Destroy the information within thirty (30) calendar days after the date of the request unless the Vendor obtains the consent of the student/individual (provided that the student is over the age of 18) or the student's parent or legal guardian to retain the PII Data; or The student/individual has transferred to another public education entity and the receiving public education entity has requested that the Vendor retain the PII Data.

H. Incident

a. Vendor shall notify the District with specific details, within one (1) calendar day after the determination that an Incident has occurred and shall cooperate with the District regarding the recovery of PII Data, Incident remediation, and the determination of whether to involve law enforcement, if any.

b. In the event an Incident involves PII Data maintained by Vendor, Vendor shall determine the cause of the

¹ C.R.S. 22-16-108 (2)



Incident and produce a remediation plan to reduce the risk of incurring a similar type of breach in the future. Vendor shall present its analysis and remediation plan to the District within thirty (30) calendar days of notifying the District of an Incident. The District reserves the right to review and adjust this plan based on best practices in data restoration and mitigation techniques such as those published by the U.S. Department of Commerce National Institute of Standards and Technology. If Vendor cannot produce its analysis and plan within the allotted time, the District, in its sole discretion, may perform such analysis and produce a remediation plan, and Vendor shall reimburse the District for the reasonable costs thereof.

c. In the event of an Incident, Vendor shall provide the District or its designated representatives with a designated point of contact for the purpose of evaluating, mitigating, or resolving the Incident, who shall respond to any contact from the District within twenty-four (24) hours of any District contact.

I. Disallowed Activities

A Vendor that uses, creates, or acquires PII Data shall not knowingly engage in any of the following activities:

- a. Vendor shall not collect, use, or share PII Data for any purpose not specifically authorized by the Agreement and DPA. Vendor may use PII Data for a purpose not strictly authorized by the Agreement and DPA only with the written consent of the District and with the written consent of the student/individual (provided that the student is over the age of 18) or the student's parent or legal guardian.
- b. Vendor shall not use PII Data in a manner or disclose PII Data to any third party that is materially inconsistent with the Vendor's privacy policy, except as stated in subsection c, below, of this Section I.
- c. Vendor may use PII Data in a manner that is inconsistent with Vendor's privacy policy without violating the terms of this Agreement and DPA for one or more of the following purposes provided that the use does not involve selling or using PII Data for Targeted Advertising or creating a personal profile of the student: (1) to ensure legal or regulatory compliance or to take precautions against liability; (2) to respond to or to participate in the judicial process; (3) to protect the safety of users or others; or (4) to investigate a matter related to public safety.
- d. If Vendor uses or discloses PII Data in accordance with Section I.3., Vendor shall notify the District within two calendar days of the use or disclosure of the PII Data.
- e. Vendor shall not sell PII Data, except in the case of the purchase, merger, or other type of acquisition of the Vendor or any assets of the Vendor by another entity, so long as the successor entity continues to be subject to the provisions of this Agreement.
- f. Vendor shall not use or share PII Data with any party for the purposes of Targeted Advertising to students. Vendor shall not use PII Data to create a personal profile of a student/individual other than for supporting the purposes authorized by the District or with the consent of the student/individual (provided that the student is over the age of 18) or the student's parent or legal guardian.

J. PII Data Security

- a. Vendor shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of PII Data. At a minimum, the information security program shall include the requirements listed in this Section J – PII Data Security.



- b. Vendor shall not share PII Data with any person who is not a Vendor, Subcontractor, or District employee on display screens, during demonstrations or presentations, or when sharing screenshots for troubleshooting or other purposes.
- c. Transparency Requirements:
 - i. Vendor shall facilitate access to and correction of any factually inaccurate student PII Data in response to a request from the District.
 - ii. Vendor acknowledges that the District may post the Vendor's name and signed Agreement date to the District's website.
 - iii. Vendor shall provide transparency to parents, school districts, and the public about its collection and use of PII by providing the following information to the District, as required to post on its public website:
 - iv. Contact information for an individual within Vendor's organization that can provide information on or answer questions related to the use of PII by Vendor. An explanation of how the PII will be shared with Subcontractors or disclosed to any third party. The types of PII that are collected, generated, or used by the Vendor. This information must include all PII that is collected regardless of whether it is initially collected or ultimately held individually or in the aggregate. An explanation of the PII, an explanation of how the PII is used, and the learning purpose for which the PII is collected and used.
 - v. Vendor shall provide updates to this information to the District as necessary to maintain accuracy.

THE PARTIES HERETO HAVE EXECUTED THIS DPA

Persons signing for Vendor hereby swear and affirm that they are authorized to act on Vendor's behalf and acknowledge that the District is relying on their representations to that effect.

Vendor

By: _____
Name of Authorized Individual

Title: _____
Official title of Authorized Individual

*Signature

District

By: _____
Name of Authorized Individual

Title: _____
Official title of Authorized Individual

*Signature