

STUDENT DATA PRIVACY ADDENDUM

COMPTON UNIFIED SCHOOL DISTRICT AND

(Consultant name as stated on W9 form)

1. Purpose of Addendum

This Student Data Privacy Addendum (“Addendum”) governs access to and obligations of the above-named Consultant (“Consultant”) with respect to Compton Unified School District (“District”) confidential student information and non-public District data disclosed to Consultant pursuant to the Services Addendum between Consultant and District entered into concurrently herewith. The purpose of this Addendum is to ensure Consultant’s compliance with all applicable federal, state, and District privacy laws, policies, and data protection requirements, including protection of personally identifiable student information.

2. Definition of Confidential Student Data

“Student Data,” as used herein, includes, but is not limited to student education records, personally identifiable information (PII), academic, behavioral, attendance, or assessment data, special education and health-related information, demographic or counseling records, digital student data and system access information, or any other information or data protected under the Data Privacy Laws, as defined below.

3. Student Data Accessed

Consultant may be provided with Student Data, in the categories set forth below, if required to perform services for the District and authorized by the District.

Authorized Data Types (check all that apply):

- Academic Records
- Attendance Information
- Demographic Data
- Special Education Information
- Student Performances/Programs
- Other: _____

4. Privacy Compliance

For purposes of this Addendum, Consultant is a “school official” with legitimate educational interests in accessing educational records. Consultant shall comply with all applicable federal and state laws and regulations pertaining to the Student Data, including, but not limited to, the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (34 CFR Part 99) (“FERPA”); Children’s Online Privacy Protection Act, 15 U.S.C. 6501-6506 (“COPPA”); Protection of Pupil Rights Amendment, 20 U.S.C. 1232h (“PPRA”); Privacy of Pupil Records, California Education Code section 49073 (“PPR”) and the Student Online Personal Information Protection Act, California Business and Professions Code section 22584 (“SOPIPA”). Collectively, the aforementioned federal and state laws and regulations shall be referred to herein as the “Data Privacy Laws.”

5. Access Authorization

Student Data shared pursuant to this Addendum shall be used only for the legitimate educational purposes described herein and/or as otherwise authorized pursuant to the Data Privacy Laws. Consultant shall not access unrelated student data, share information with unauthorized individuals or organizations, sell, distribute, or repurpose student information. Consultant acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including, without limitation, metadata, user content, or other non-public information and/or personally identifiable information contained in the Student Data, without the express prior written consent of the District.

Consultant must secure electronic devices and maintain password protection, use encrypted storage or secure District systems when applicable, protect physical documents from unauthorized access in accordance with industry standards, and immediately report lost devices or potential data breaches in

accordance with this Addendum. Consultant shall ensure its personnel, including employees, officers, directors, and subcontractors, shall comply with the terms of this Addendum. Consultant is expressly prohibited from using any Student Data to engage in targeted advertising. In the event of a subpoena or legal process requiring disclosure, Consultant shall notify the District within forty-eight (48) hours (or sooner if required) to allow the District to assert any applicable rights.

6. Data Ownership

All Student Data transmitted to the Consultant pursuant to this Addendum is and will continue to be the property and under the control of the District. Consultant further acknowledges and agrees that all copies of such Student Data transmitted to Consultant, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Addendum in the same manner as the original Student Data.

7. Disposition of Student Data

Upon completion or termination of services, Consultant shall return all Student Data to the District, or securely destroy all physical and electronic Student Data, and certify destruction upon District request.

8. Parent, Guardian, or Employee Request

Consultant shall refer any parent, guardian, employee, or third party to the District for any request to review or access Data in the District's possession. The District will follow the necessary and proper procedures to respond to any such request as required by law.

9. Notice of Breach

Any suspected data breach, unauthorized disclosure, or privacy concern must be reported within twenty-four (24) hours to the District contact listed above. Consultant shall report: (1) the nature of the unauthorized use or disclosure; (2) the Data used or disclosed; (3) who made the unauthorized use or received the unauthorized disclosure; (4) what Consultant has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and (5) what corrective action Consultant has taken or shall take to prevent similar unauthorized use or disclosure.

10. Indemnification

To the furthest extent permitted by California law, Consultant shall, at its sole expense, defend, indemnify, and hold harmless the District, its agents, representatives, officers, employees, volunteers, and trustees ("Indemnified Parties") from any and all demands, losses, liabilities, claims, suits, and actions (the "Claims") of any kind, nature, and description, including, but not limited to, personal injury, death, property damage, and consultants and/or attorneys' fees and costs, directly or indirectly arising out of, connected with, or resulting from the performance of this Addendum, including failure to properly safeguard Student Data, unless the claims are caused wholly by the gross negligence or willful misconduct of the Indemnified Parties.

11. Miscellaneous

All provisions and obligations of the Data Privacy Laws shall be read into and required by this Addendum as though those provisions and obligations were expressly stated in this Addendum. Failure to comply with this Addendum may result in immediate termination of services or contract, removal of data access privileges, legal action and penalties permitted by law, and reporting to applicable oversight agencies. This Addendum shall be governed by and the rights, duties and obligations of District and Consultant shall be determined and enforced in accordance with, the laws of the State of California and within Los Angeles County.

Consultant Name (Print): _____

Signature: _____

Date: _____