STUDENT DATA PRIVACY AGREEMENT

August 28, 2019

This Student Data Privacy Agreement ("DPA" or "Agreement") is effective as of September 1, 2019, by and between the Santa Rosa City Schools (hereinafter referred to as "LEA"), University of Texas at Austin's Population Research Center (hereinafter referred to as "Provider") (collectively, "Parties") on the terms as stated herein.

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data transmitted to Provider from LEA, including compliance with all applicable state and federal laws as they may be amended from time to time. In performing its obligations under this Agreement, the Provider shall be considered a "school official" with a "legitimate educational interest" and performing services otherwise provided by LEA employees, as those terms appear in 34 C.F.R. § 99.31(a)(1)(i)(B). With respect to the use and maintenance of Student Data, Provider shall solely act under the direct control and supervision of LEA.

2. **Nature of Services Provided.** This Agreement applies to the following specified services: high school transitional interventions to improve students' academic outcomes and social success during high school and beyond and longitudinal research to assess effectiveness and improve academic offerings ("Services").

3. **Student Data to Be Provided**. Provided full and ongoing compliance with all of the obligations in this Agreement, without limitation, Santa Rosa City Schools will transfer to Provider course- taking and grades data, final transcripts, graduation status, attendance records, test scores (e.g., state tests, College Board data, ACT data), and certain post-graduation information pertaining to students belonging to the 2015-2016 freshman class at Piner High School. The Parties shall indicate the categories of student data to be provided in the Data Schedule, attached hereto as Exhibit "A".

4. **DPA Definitions.** Certain definition of terms used in this DPA are found in Exhibit "B".

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Property\Data Control as between LEA and Provider**. The Parties agree that as between them, all rights in Student Data shall remain the property of the LEA. At all times, all LEA student records shall remain under LEA's control.

2. **Parent Access.** The Parties shall develop, update, and publicize reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data held by Provider and correct erroneous information, in compliance with California Education Code § 49070. Provider shall respond in a timely manner (and no later than 15 calendar days from the date of the request) to the LEA's request for Student Data held by the Provider to

view or correct as necessary. In the event that any individual, including the parent of a pupil, contacts the Provider to review any of the Student Data held by Provider pursuant to the Services, the Provider shall refer the parent or individual to the LEA, which will then follow its own procedures regarding the request.

3. **Third Party Request.** Should a third party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the third party to request the data directly from the LEA. Provider shall notify the LEA in advance of any legally compelled disclosure to a third party.

ARTICLE III: DUTIES OF LEA

1. **Reasonable Precautions: Credentials**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services.

2. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. Provider will assist all LEA's efforts to investigate and respond to any such unauthorized access.

ARTICLE IV: DUTIES OF AND RESTRICTIONS ON PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security.

2. **Prohibitions on Use.** Any Student Data available to Provider, including its own identifiers, shall not be used for any purpose other than the Services stated in Article 1, Section 2, above.

3. **No Redisclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, metadata, Pupil Generated Content, non-public information and/or Personally Identifiable Information contained in the Student Data.

4. **De-identified Information.** De-identified Information may be used when consistent with federal law. Provider agrees not to attempt to re-identify De-identified Information.

5. **Deletion of Student Data.** Provider shall delete all Student Data obtained under this Agreement at the time it is no longer needed for the purpose for which it was obtained. Upon Termination of this Agreement, Provider shall delete all Student Data obtained under this Agreement. Deletion shall include the shredding of any hard paper copies containing any Student Data and deletion of all digital copies of Student Data. Provider shall provide written notification of deletion to LEA upon LEA's reasonable request.

6. **Targeted Advertising Prohibition.** As provided in California Education Code § 49073.1, Provider is prohibited from using or selling Student Data to:

(a) market or advertise to anyone, including students or family members/guardians;
(b) inform, influence, or enable marketing, advertising, or other commercial efforts by Provider;
(c) develop any profile of a student or family member/guardian; or
(d) use the Student Data for the development of commercial products or services.

ARTICLE V: DATA SECURITY AND PROTOCOLS FOR UNAUTHORIZED ACCESS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures. Consistent with industry standards and technology best practices, the parties shall work together to protect Student Data from unauthorized disclosure or acquisition by any unauthorized person. The general security duties of Provider shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall provide access to Student Data to employees or contractors who are performing the Services and to no other persons, provided any employees or contractors with access to Student Data shall have passed a criminal background check and shall have signed a written certification that they have read this Agreement and will abide by all restrictions and prohibitions on use specified herein as well as a confidentiality agreement.

    b. **Security Protocols.** Provider agrees to maintain security protocols that meet industry standards in the transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by persons legally allowed to do so. Provider shall maintain all Student Data in a secure environment and not copy, reproduce, or transmit Student Data, except as necessary to fulfill the purpose of the Services.

    c. **Employee Training.** Provider shall conduct periodic security training to those of its employees or contractors who operate or have access to its system. Further, Provider shall designate an employee for LEA to contact if there are any security concerns or questions and provide LEA with that designee's contact information.

    d. **Security Technology.** When the Services are accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access, including server authentication and data encryption.

    e. **Sub-processors Bound.** Provider shall require of any Sub-processors who access Student Data that they first agree in writing to secure and protect Student Data and restrict any uses of Student Data to those consistent with Provider's own obligations specified herein. The Parties shall periodically conduct or review compliance monitoring and assessments of Sub-processors to determine their compliance with this Agreement.

    f. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct

periodic (no less than semi-annual) risk assessments of the digital and physical environment where it stores or otherwise handles Student Data and to expeditiously remediate any identified security and privacy vulnerabilities upon identification.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, not to exceed twenty-four (24) hours. In furtherance of this obligation, Provider shall comply with the following notification process:

   a. The notification shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) date and time the incident was discovered; (4) nature of the incident (e.g., system level electronic breach, an electronic breach of one computer or device, or a breach of hard copies of records; (5) a description of the information lost or compromised; (6) name of electronic system and possible interconnectivity with other systems; (7) storage medium from which information was lost or compromised; (8) controls in place to prevent unauthorized use of the lost or compromised information; (9) number of individuals potentially affected; and (10) whether law enforcement has yet been contacted.

   b. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in subsection (a) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

   c. If, after the initial report, additional information baring on any of these topics becomes known to Provider, Provider shall send an updated report within one day of receiving the new information.

   d. Provider agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, all procedures for notification and mitigation of any such data breach.

   e. Provider further acknowledges and agrees to prepare a written incident response plan upon entering this Agreement consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, and agrees to provide LEA, upon request, with a copy of said written incident response plan.

   f. Provider is prohibited from directly contacting any parent, legal guardian or

eligible pupil unless expressly requested by LEA. Provider shall notify the affected parent, legal guardian or eligible pupil (of majority age) of the unauthorized access, which shall include the information listed in this Article, above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

ARTICLE VI: NO PUBLICATION OF STUDENT DATA

Should the Provider present, publish, or use student results it has gained in the course of its analysis, publications and reports of data and information shared, including preliminary descriptions and draft reports, shall involve only aggregate or de-identified data and no personally identifiable information or other information that could lead to the identification of any student, parent, or teacher

ARTICLE VII: MISCELLANEOUS

1. **Term.** Provider shall be bound by this DPA for as long as the Provider maintains any Student Data.

2. **Termination.** LEA shall have the at-will right to terminate any obligation to grant Provider access to any Student Data or to grant Provider ongoing authority to maintain Student Data collected under this Agreement.

3. **Effect of Termination on Survival.** Provider's obligations under Articles IV, V, and VII shall survive any termination. If Pupil Generated Content is stored or maintained by the Provider as part of the Services described in Exhibit "A," Provider shall, only upon an express request by LEA, transfer said Pupil Generated Content to a separate student-controlled account upon termination of this Agreement; provided, however, such transfer shall only apply to Pupil Generated Content that is severable from the Service. After this Pupil Generated Content is transferred to the LEA, the Provider shall destroy all of LEA's Student Data.

4. **Notice and Designated Representatives.** All notices or other communication required or permitted to be given hereunder must be in writing and sent via first-class mail, postage prepaid, to the designated representatives below (and by e-mail transmission only if an email address is provided below):

Designated Representatives

The designated representative for the LEA is:

Name: Rick Edson
Title: Deputy Superintendent

Contact Information (include email address if electronic notice is adequate):

_____

_____

_____

The designated representative for the Provider is:

Name:_____
Title: _____

Contact Information (include email address if electronic notice is adequate):

_____

_____

_____

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction.**

THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA, INCLUDING WITH REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF SONOMA, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY. THE PARTIES ACKNOWLEDGE THAT NOTHING IN THE AGREEMENT SHALL CONSTITUTE A WAIVER OF SOVEREIGN IMMUNITY BY PARTIES THAT ARE STATE AGENCIES.

7. **Indemnification.**

Provider shall indemnify and hold LEA harmless from liability resulting from the negligent acts or omissions of Provider, its agents or employees pertaining to the activities to be carried out pursuant to the obligations of this Agreement; provided, however, that Provider shall not hold LEA harmless from claims arising out of the negligence or willful malfeasance of LEA, its officers, agents, or employees, or any person or entity not subject to Provider's supervision or control.

LEA shall indemnify and hold Provider, their Regents, officers, agents and employees harmless from liability resulting from negligent acts or omissions of LEA pertaining to the activities to be carried out pursuant to the obligations of this Agreement, including but not limited to the use by LEA of the results of the Study; provided, however, that LEA shall not hold Provider harmless

from claims arising out of the negligence or willful malfeasance of LEA, its officers, agents, or employees, or any person or entity not subject to LEA's supervision or control.

8. **Authority.** This agreement is subject to LEA's bylaws and board policies for designating authority to execute contracts on the LEA's behalf. Provider represents that it is authorized to bind itself to the terms of this Agreement, including without limitation destruction of Student Data, and on behalf of all related or associated institutions, individuals, employees, and/or contractors who may have legal access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

9. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right, and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

10. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

11. **Amendment**. This Agreement cannot be changed or supplemented orally and may only be modified or superseded by written instrument executed by both Parties.

IN WITNESS WHEREOF, the parties have executed this Data Privacy Agreement as of the last day noted below.

Provider:

BY:_____ Date:_____

Printed Name:_____ Title/Position:_____

Local Education Agency:

BY:_____ Date:_____

Printed Name: Rick Edson Title/Position: Deputy Superintendent

Note: Electronic signature not permitted.

EXHIBIT "A"

DATA SCHEDULE

Student Demographics

a) School year
b) Student ID
c) School Name
d) Date of birth
e) Enrollment status (at end of school year)
f) Gender
g) Race/Ethnicity
h) Free and Reduced Lunch Status
i) Graduation Status (when available in summer)

Student Achievement/ Course Tracking/Transcript

a) Term (fall/spring semester or trimester or quarters as applicable)
b) School Name
c) Grade Level
d) Course Name
e) Course ID
f) Final Course Grade/Mark (Outcome)
g) Credits earned
h) Teacher First Name
i) Teacher Last Name
j) Cumulative GPA unweighted
k) Cumulative GPA weighted

ACT

a) School Name
b) Exam Type
c) Date Exam Taken
d) Composite Score
e) English score
f) Math score
g) Reading score
h) Science score
i) Writing score

Student State Assessment/EOC

a) Mathematics
a. Name of Test
b. Scale Score
c. Raw Score
d. Standard Met

b) Reading/Writing
a. Name of Test
b. Scale Score
c. Raw Score
d. Standard Met

c) Science
a. Name of Test
b. Scale Score
c. Raw Score
d. Standard Met

d) Social Studies
a. Name of Test
b. Scale Score
c. Raw Score
d. Standard Met

College Board (Pre-AP/AP)

a) AP Exam Date
b) AP Exam Subject
c) AP Exam Score

PSAT/ NMSQT/SAT

a) School Name
b) Exam Type
c) Date Exam Taken
d) Critical Reading (taken January 2016 or prior) score
e) EBRW Reading (taken March 2016 or later) score
f) Writing (2016 or prior) score
g) EBRW Writing & Language score
h) Math score
i) Essay score

EXHIBIT "B"

DEFINITIONS

De-Identified Information. De-Identified Information is given the same definition as appears in California Education Code § 49073.1(d)(1).

"Personally Identifiable Information" or "PII": "Personally Identifiable Information" or "PII" shall include all categories of data falling under the definition of "Personally identifiable information" set forth in Santa Rosa City School's Administrative Regulation 4040.

Pupil Generated Content is given the same definition as appears in California Education Code § 49073.1 (d)(4).

Student Data: Student Data includes without limitation any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of any student that has ever been enrolled at LEA including, but not limited to, information in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs, as well as any such student's email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings, geolocation information, or Pupil Generated Content. Student Data shall not include De-Identified Information.

Sub-processor: "Sub-processor" means a party other than LEA or Provider, in a contractual relationship with Provider for data processing, collection, storage, or other related service so Provider may operate and/or improve the Services, and that has access to PII.