

**SAN DIEGO COUNTY SUPERINTENDENT OF SCHOOLS
6401 Linda Vista Road
San Diego, California 92111**

MEMORANDUM OF UNDERSTANDING FOR DATA SHARING SERVICES

This Memorandum of Understanding (“MOU”) is entered into this 1st day of July 2019 through June 30th, 2022 by and between the SAN DIEGO COUNTY SUPERINTENDENT OF SCHOOLS (“SDCOE”) and the San Pasqual Union School District (“LEA,” together with SDCOE, the “Parties”).

WHEREAS, SDCOE and LEA enter into this MOU to facilitate the mutual sharing of data and establish responsibilities between the Parties; and

WHEREAS, the Parties wish to protect the privacy of pupil records, and to comply with any applicable privacy statutes, including the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99, as amended; “FERPA”); California Education Code § 49073.1; the Student Online Personal Information Protection Act (California Business and Professions Code § 22584; “SOPIPA”); California Civil Code § 1798.29; and California Government Code § 6250 et seq.; and

WHEREAS, the purpose of this MOU is to set forth the rights and responsibilities of SDCOE and LEA with respect to data collected or retained by LEA or by SDCOE pursuant to this MOU.

NOW THEREFORE, in consideration of the terms and conditions hereof, including the recitals, the Parties agree as follows:

1. Role of SDCOE

1.1 SDCOE shall provide services designed to assist LEA with certain requirements and mandates for managing or reporting on data collected by LEA, potentially including the integration of data between disparate systems, and staff and pupil records, which include any information that is directly related to a student that is maintained by LEA or acquired directly through the use of instructional software or applications assigned to a student by a teacher or other LEA employee (collectively, “Data”). Services rendered under this MOU shall be referred to as “Core Services” and be identified in Exhibit A hereto.

The LEA may request in writing to opt into participation in one or more core services outlined in Exhibit A. SDCOE reserves the right to accept or deny such request for services. Once this decision is made, SDCOE shall provide a written response to the LEA either accepting or denying the request within 10 working days of receipt of the request to add services.

2. Responsibilities of SDCOE

SDCOE will provide any services it delivers in a timely and professional manner.

2.1 SDCOE will ensure any systems it develops with such Data to serve the needs of LEA or public agencies will have appropriate levels of security, as further detailed in Section 11 (Data Security) of this MOU.

2.2 SDCOE shall help ensure Data available can only be viewed or accessed by agencies legally allowed to do so, and as agreed upon by LEA and SDCOE.

2.3 Should it be deemed necessary, SDCOE will specify and assist in allowing network access to resources, in a controlled and secure manner.

3. LEA Rights and Responsibilities

LEA shall provide system linkages or necessary Data extracts or permission access from LEA's student information or other systems on an agreed upon or pre-defined schedule between the Parties. Any such schedule agreed upon in writing (including email) between the Parties shall be deemed incorporated herein and made a part hereof upon such mutual agreement.

3.1 Data extracts will be provided through secure electronic transmission by LEA to SDCOE.

3.2 LEA will be responsible for providing the data needed to integrate LEA's Data into SDCOE's data repositories as needed to perform the required tasks.

3.3 Data provided by LEA shall include Data relevant to the purpose of this MOU or specific system requirements.

3.4 LEA shall be responsible for determining which of their staff has access to system, communicating to SDCOE the roles and responsibilities of each person with said access, including the person who is responsible for maintaining LEA's main and sub-accounts, and communicating the names of individuals for whom access should be removed due to change of position or separation from the LEA.

3.5 LEA shall designate those individuals who can: (a) transmit Data to SDCOE; (b) request release of Data to LEA or third parties; or (c) request extracts or analysis of LEA's Data.

4. Third-Party Agencies

Third parties may include but are not limited to public agencies the Parties desire to collaborate with, public agencies the Parties are required to share Data with, and/or any third-party vendor of either Party. Permission for SDCOE to share Data with a third party must be first granted by LEA in writing.

5. Amendments to MOU

The MOU shall be supplemented by amendments or other attachments that will reflect specific undertakings by SDCOE and LEA.

6. Applicable Law

6.1 Data sharing under this MOU will from time to time include SDCOE collecting and maintaining educational, personnel, medical and financial records that contain personally identifiable information (PII) on students or staff of LEA. SDCOE is bound by the same regulations and laws for access and management of this Data, and will conform to all legal requirements. SDCOE and LEA agree that the disclosure of information under this MOU complies with the requirements of Education Code § 49073 et seq., FERPA, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), SOPIPA, and other state and federal/European Union laws and regulations regarding educational, personnel, medical and financial records.

6.2 The Parties understand that certain federal and state programs and laws, including the free and reduced lunch program and laws governing the provision of special education services, have additional legal requirements for data security, and both Parties agree to maintain full compliance with such requirements. Without limitation to the foregoing, SDCOE and LEA additionally agree that aggregated (non-individually identifiable) and non-aggregated PII Data may be reported upon or shared as allowable by law.

6.3 SDCOE and LEA shall ensure joint coordination and cooperation with one another to ensure compliance with FERPA, 20 U.S.C. § 1232g; 34 C.F.R. Part 99, as amended. The foregoing notwithstanding, SDCOE and LEA agree that LEA shall be responsible for providing notices to parents required under FERPA, obtaining necessary parental consent required under FERPA, and for providing parent(s), guardian(s) or student(s) with an opportunity to inspect and challenge the contents of Data shared with SDCOE pursuant to this MOU.

7. Ownership of Data

SDCOE and LEA agree that LEA will continue to maintain ownership of and control over its source Data. SDCOE agrees that it will not alter LEA's source Data without explicit authorization from LEA, and is not responsible for any errors therein. SDCOE shall not be responsible for the type or quality of the Data provided by LEA, and SDCOE makes no warranty as to the Data itself. LEA understands that though SDCOE may notify it of issues it discovers with the source Data, LEA is responsible for any corrections required to its own Data or will authorize SDCOE to make any limited explicit changes. LEA acknowledges that accurate reports rely upon accurate source Data being maintained by LEA. Each party owns or controls its data systems and the work product generated by such systems.

8. Prohibited Use of Data

Except as otherwise permitted by the terms of this MOU, SDCOE shall not use the Data supplied to it in an unauthorized manner. Specifically, SDCOE shall not sell or release Data, nor enable or permit third parties to engage in targeted advertising to students or to build student profiles unrelated to the purposes contemplated by this MOU.

9. Student and Parent Access to Data

SDCOE shall work with LEA to provide a means by which employees, when authorized by LEA, can search and access student Data through reasonable procedures for LEA to respond to a parent, legal guardian, or eligible student who seeks to review PII in the pupil's records and to correct erroneous information. The foregoing notwithstanding, SDCOE shall cooperate with LEA to help ensure this record correction will be consistent with LEA's policies regarding record correction.

10. Third-Party Vendors

SDCOE will have contracts with third parties to help SDCOE maintain the SDCOE data system ("SDCOE Contractors"). SDCOE may not distribute student or staff Data to any SDCOE Contractors without LEA's written consent or as permitted by this MOU, unless required by law. SDCOE shall ensure that approved subcontractors adhere to this MOU. SDCOE will help ensure that any subcontractor or sub-processor that it engages, to process, store, or access Data, has adequate technical security and organizational measures in place to keep Data secure and comply with this MOU. SDCOE will require any third-party vendors and subcontractors to comply with any applicable state and federal laws and regulations regarding educational records and data privacy, including but not limited to: Education Code §§ 49073.1, 49076, and 49076.5; FERPA; HIPAA; and SOPIPA.

11. Data Security

Both Parties agree to maintain appropriate security protocols in the transfer or transmission of Data, including ensuring Data may only be viewed or accessed by Parties legally allowed to do so. SDCOE shall maintain Data obtained or generated pursuant to this MOU in a secure computer environment and not copy, reproduce, or transmit Data obtained pursuant to this MOU, except as requested by LEA. SDCOE shall provide security training to those of its employees who operate or have access to the system. SDCOE may also provide an initial security training to LEA. SDCOE shall provide LEA with contact information for the person at SDCOE who

LEA may contact if LEA has security concerns or questions. Where applicable, SDCOE will require unique account identifiers, user names, and passwords that must be entered each time a client or user signs in. A description of SDCOE's data security practices and procedures is attached to this MOU as Exhibit B.

12. Data Breach Notification

SDCOE shall maintain Information Security & Privacy Insurance with Electronic Media Liability policy with coverage limits of no less than one million dollars (\$1,000,000.00) per occurrence and five million dollars (\$5,000,000.00) aggregate for the duration of this MOU. Such policy shall cover damages resulting from the unauthorized access to, or theft of, data obtained by SDCOE in connection to this MOU, as well as the unauthorized disclosure or use of (PII) that SDCOE may acquire from LEA ("Data Breach"). It is further agreed and understood that the policy shall include coverage for crisis management costs, credit-monitoring expenses, payment of monies requested in connection to cyber extortion of LEA Data, and defense costs, fines, and penalties related to a Data Breach. Parties agree that the insurance requirements referred to herein shall apply to any third-party vendors hired by SDCOE that may obtain or maintain LEA Data, as well as the outside agencies referred to in Section 0 of this MOU. LEA reserves the right to request proof of insurance from SDCOE, third-party vendors, and outside agencies to confirm compliance with these insurance requirements. Upon becoming aware of any unlawful or unauthorized access to student or staff Data stored on equipment used by SDCOE or in facilities used by SDCOE, SDCOE will take the following measures:

12. Promptly file a claim with SDCOE's Information Security & Privacy Insurance with Electronic Media Liability policy provider.

12.2 Promptly notify LEA of the suspected or actual incident, including the type of Data subject to unauthorized access.

12.3 Promptly investigate the incident and provide LEA with detailed information regarding the incident, including the identity of the affected users, and the estimated date of the breach.

12.4 Assist LEA in notifying either the student or their legal guardian, and take commercially reasonable steps to mitigate the effects and to minimize any damages resulting from the incident.

13. Outside Agencies

13.1 SDCOE may be required by subpoena or other lawfully issued order to divulge Data to law enforcement or another agency. When permitted by the requesting agency, SDCOE shall provide LEA with notice of the request and types of information requested. Both SDCOE and LEA have periodic needs to share Data, as legally allowed, with public agencies needing access to such Data to provide services to students. SDCOE and LEA understand that sharing Data for use in such systems streamlines the process of providing services to students. SDCOE agrees that no Data will be made accessible to any such agency for any purpose other than those limited to the Data required and only under conditions allowed by law. Education Code §§ 49076 and 49076.5, as amended, and 20 U.S.C. § 1232g and 34 C.F.R. § 99.31, as amended, provide specific conditions under which Data may be accessed by or shared with public agencies.

13.2 SDCOE may have periodic needs to share Data, as legally allowed, with university researchers for academic purposes to allow university researchers to collaborate with LEA and SDCOE or to perform relevant research studies. SDCOE shall notify LEA in writing of any Data sharing pursuant to this Section, as follows:

1. Describe the identity of the researchers/organizations to whom the Data will be transmitted

2. Provide contracts when requested, which shall include provisions binding the researcher/organization to the terms of this MOU
3. Describe the types of Data to be transmitted
4. Describe the manner in which the Data shall be de-identified or aggregated.

14. Independent Contractors

Both Parties may engage the services of outside professionals in the course of administration, development or technical support of data systems. Any such professionals will be bound at all times by the same confidentiality and security requirements which are applicable to any data within the Parties' systems, and by state and federal law governing such access.

15. Indemnification and Liability

Each Party agrees to indemnify the other against any and all liability, actions, claims, damages, losses, costs, and expenses (including attorneys' fees) arising out of or in any way resulting from the indemnifying Party's own negligent or intentional acts, errors, or omissions in connection to the performance of the responsibilities of each Party, per this MOU. The Parties shall not be held liable for any special, consequential, indirect or incidental damages incurred as a result of this MOU. The Parties shall be held harmless for any claims or lawsuits arising out of the release of information pursuant to a request by one of the Parties in conformity with this MOU or pursuant to law, excluding such release in connection to the negligence of either Party, or that of its officers, agents, or employees. If liability, damages, or any other claim relating to Data shared pursuant to this MOU is a result of a third party's act or omission, then the indemnification and defense that the third party contractually owes to SDCOE and/or LEA shall also be extended to the other Party to this MOU, to the maximum extent possible.

16. Severability

If any provision of this MOU is determined by a court to be invalid, unenforceable or otherwise ineffective, that provision shall be severed from the rest of this MOU, and the remaining provisions shall remain in effect and enforceable.

17. Term

This MOU may be periodically or annually updated to incorporate changes if required upon mutual agreement of the Parties. LEA understands that this MOU is part of an effort to standardize data sharing and management between SDCOE and all districts it serves, and as such, every effort will be made to maintain a common agreement across all agencies. Notwithstanding the foregoing, this MOU shall terminate effective June 30, 2022.

18. Termination

Either Party may terminate this MOU upon ninety (90) days' written notice. Upon termination or expiration of this MOU, SDCOE shall work with LEA for the orderly cessation of extracts of student Data. Upon termination or expiration of this MOU, SDCOE shall return or delete personally identifiable student Data unless otherwise provided by law or mutual agreement of the Parties. SDCOE and LEA understand that SDCOE may have an ongoing need to reference the raw Data it acquired during the term of this MOU. In the event that such need arises, SDCOE shall, to the extent possible and subject to the mutual agreement of the LEA, only retain anonymized, aggregated Data that it obtained from LEA during the term of this MOU. However, SDCOE certifies

that such anonymized, aggregated Data shall be purged when the Data has exceeded its useful life and shall not be kept for more than seven (7) years unless otherwise legally required.

19. Dispute Resolution

In the event of a dispute between any Party to this MOU, the parties shall attempt to resolve their disputes informally, in discussions involving the decision- makers for each of the parties. If these discussions are not successful, the parties shall retain a mediator to resolve the dispute with the mediation to be held within ninety (90) days of the date the dispute arises. If mediation is not successful, either party shall have the right to bring the dispute before the San Diego County Superior Court.

IN WITNESS WHEREOF, the Parties agree to this Memorandum of Understanding to be executed by their duly authorized officers in the County of San Diego, State of California.

SAN DIEGO COUNTY OFFICE OF EDUCATION

SAN PASQUAL UNION SCHOOL DISTRICT

By: _____

Name: Mr. Michael Simonson

Title: Chief Business Officer, Deputy Superintendent
San Diego County Office of Education

Dated: _____

By: _____

Name: Dr. Terry Loftus

Title: Chief Technology Officer
Assistant Superintendent Integrated
Technology Services

Dated: _____

By: _____

Name: _____

Title: _____

Dated: _____

EXHIBIT A

SDCOE Core Services

Service Provider	Application/ Project Name	Division/ Department	Ed Code 49073.1(a)	Employee Information	HIPAA / Medical Info
<p>National Student Clearinghouse</p> <p>The LEA and SDCOE agree to collaborate in order to maximize student preparation for college and career during the K-12 experience. In order to accurately track the progress of San Diego county high school graduates' success in post-secondary education and to be able to adjust programs and services to maximize student success in such institutes, we have established a MOU regarding the use of StudentTracker, a tool developed by the National Student Clearinghouse.</p>	<p>Student Tracker</p> <p>The LEA upon participation submits accurate, updated data for each high school (periodically and as appropriate) to StudentTracker guidelines for submission to the National Student Clearinghouse.</p>	LLS/AAE	YES	NO	NO
<p>CORE Districts/ Education Analytics</p> <p>The CORE Districts and their analytic partner Education Analytics serves together to maximize the use of data to populate dashboards associated with the CORE Data Collaborative. At the request of SDCOE and under the Joinder agreement with CORE, Education Analytics may supply additional analytical support and data extracts to LEAs in support of their</p>	<p>Data Collaborative/Dashboard / Predictive Analytics</p>	LLS/AAE ITS/ITS	YES	NO	NO

Service Provider	Application/ Project Name	Division/ Department	Ed Code 49073.1(a)	Employee Information	HIPAA / Medical Info
<p>analysis of student data trends and/or LEA participation in predictive analytics projects. Data provided to SDCOE may also be leveraged to support the LEA with data visualizations and the development of dashboards through the use of platforms including Power BI and Tableau.</p>					
<p>SDCOE LLS/MEGA</p> <p>SDCOE shall provide the MEGA dashboard to support the LEA in understanding and monitoring the progress of language learners. The MEGA Dashboard is a tool that utilizes business intelligence software, establishing a dynamic, multi-faceted assessment system to monitor the progress of language learners. This tool provides visualizations of both academic and linguistic data and assists districts.</p> <p>Data provided to SDCOE may also be leveraged to support the LEA with data visualizations and the development of dashboards through the use of platforms including Power BI and Tableau.</p>	<p>MEGA EL Dashboard</p> <ul style="list-style-type: none"> · Provide data monitoring for students including English learners. · Monitor progress towards reclassification at the student level · Monitor the progress of reclassified students per CDE requirements · Provide LCAP metrics 	<p>ITS/ITS</p>	<p>YES</p>	<p>NO</p>	<p>NO</p>
<p>Ed-Fi/Digital Promise In coordination with third party services providers or grantors</p>	<p>SDCOE Data Interoperability</p>	<p>LLS/ITS/ Innovation</p>	<p>YES</p>	<p>NO</p>	<p>NO</p>

Service Provider	Application/ Project Name	Division/ Department	Ed Code 49073.1(a)	Employee Information	HIPAA / Medical Info
<p>including the Ed-Fi Alliance and/or Digital Promise SDCOE shall provide the LEA metrics output from combined data sets, utilizing the Ed-Fi data structure to combine student information system data with one or more additional sources of data. The LEA shall provide any additional sources of data through either data submissions through secure transfer or via APIs to subscription software as services the LEA has contracted with.</p> <p>Data provided to SDCOE may also be leveraged to support the LEA with data visualizations and the development of dashboards through the use of platforms including Power BI and Tableau.</p>					

EXHIBIT B**SDCOE Data Security Practices and Procedures**

Introduction: SDCOE has established an Information Security (InfoSec) Program based on industry best practices and the needs of California K12 systems. The InfoSec program involves several departments, including Operational Support Services, Personnel Services, and Information Technology Services. The departments are primary functional units that will engage with legal counsel and security service/solution providers to develop and execute improvement plans. This plan may be periodically updated to take into account improving practices and technologies and to respond to a changing threat environment. LEA's will be provided with annual updates where there have been material modifications to the practices and procedures stated below.

As of January 1, 2019, the Program has identified the following areas to be part of the continual improvement of the SDCOE InfoSec practices.

1. **Anti-Virus/Malware Administration and Configuration**
 - a. Regularly review and examine the policies and procedures related to Anti-virus/Malware controls and the configuration of Anti-virus/Malware software and appliances
 - b. Continual improvement of Anti-virus/Malware software configuration, operation and security
 - c. Provide Anti-virus/Malware training and awareness
 - d. Practice in depth Anti-virus/Malware defense for server and end user computers

2. **Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP)**

COOP is the collection of sets of processes and procedures carried out by an organization to ensure that essential business functions continue to operate during and after a disaster. As part of the COOP there is a **DRP**. These are the technical plans developed for specific groups within an organization to allow them to recover a particular business application. SDCOE addresses these plans by:

 - a. Performing annual Business Impact Analysis with various departments to identify mission critical processes and/or departments and prioritize the recovery processes and/or departments in accordance with their level of criticality.
 - b. Secure Executive Oversight and Support for the COOP
 - c. Continual updates of documentation, content, sufficiency, testing and documentation of test results of the plans.

3. **Firewall Administration and Configuration**
 - a. Examine and document the policies and procedures related to the administration of the organizations firewall(s)
 - b. Examine and document configuration files and access control lists for the devices and/or applications and operating systems
 - c. Implement least privilege access
 - d. Documentation, content and sufficiency of firewall policies and procedures
 - e. Logical placement of firewalls
 - f. Restricted access to management interfaces
 - g. Continual evaluation of applied rule sets
 - h. Backup, recovery, and storage of configuration files
 - i. Firewall event log review and sufficient storage for retention policy

4. **Network Systems and Database Vulnerability Scanning**

Perform scheduled simulations of attacks on the network and database systems by utilizing industry best of breed tools, which identify the vulnerabilities in the systems and provide recommendations for remediation.

5. Network Monitoring & Intrusion Detection

- a. Regularly review the event logs to identify and correlate unauthorized, unusual, and sensitive access activity, such as:
 - 1. Attempted unauthorized logical and physical access;
 - 2. Access trends and deviations from those trends;
 - 3. Access to sensitive data and resources;
 - 4. Highly-sensitive privileged access, such as the ability to override security controls;
 - 5. Access modifications made by security personnel; and
 - 6. Unsuccessful attempts to logon to a system.
- b. Improve documentation, content and sufficiency of network monitoring and intrusion detection policies and procedures

6. Patch Management

- a. Regularly review and update systems, configuration, and applications for required systems
- b. Sufficient testing of systems before and after patching
- c. Maintain documentation of patch history of required systems

7. Physical Security

To prevent unauthorized personnel from gaining direct access to SDCOE facilities that house sensitive information, the following areas are under regular review and improvement process:

- a. Documentation, content and sufficiency of physical security policies and procedures
- b. External: facility perimeter, perimeter lighting, parking areas, parking area lighting, landscaping, exterior building lighting, exterior doors and locks and other entry points
- c. Internal: doors, windows, ceilings, raised floors, wiring and utility closets, ceilings, attics, basements, crawlspaces, public areas
- d. Lock and Key control
- e. Access control including identification systems in use and access points
- f. Intrusion alarms
- g. Fire detection, suppression and prevention
- h. CCTV/digital imaging technologies
- i. Power system and utility control points
- j. Documentation, retired network storage, and refuse disposal
- k. Mail Handling
- l. Hard copy record storage
- m. Network Operations Center

8. Server (Data Center Systems) Administration and Configuration

Continual improvement of the following areas:

- a. Documentation of server implementations, policies, and procedures
- b. Hardware, operating system, and application security
- c. User account policy and rights assignments
- d. Auditing policies, system changes, user rights, and access to sensitive data
- e. Event and security log retention and regular review
- f. Critical file and folder permissions
- g. Remote access and security

9. Network Switch and Router Administration and Configuration

Continual improvement of the following areas:

- a. Develop clear documentation, content and sufficiency of policies and procedures
- b. Streamline installation, operation and security
- c. Regular review of configuration

10. Workstation Administration and Configuration
Continual improvement of the following:
 - a. Documentation of workstation policies and procedures
 - b. Hardware security
 - c. Operating System installation, configuration and maintenance (patching)
 - d. User account policies and rights assignments
 - e. Event and security log settings and retention
 - f. Critical file and folder permissions
 - g. Remote access and security

11. Mobile Devices
Regularly examine SDCOE's policies and procedures related to administration of the mobile devices assigned to staff and students. The mobile devices include laptops, tablets and smartphones for both SDCOE owned devices and personal devices brought onto SDCOE's network.

12. Application Security Assessment and Mitigation
The primary objective is to assess how effectively and efficiently SDCOE ensures that no single trusted IT system user, administrator, or vendor is able to exploit vulnerabilities in SDCOE's IT systems to accomplish and/or conceal an unauthorized diversion of SDCOE's assets. Identify where the risk exists and evaluate the controls designed to mitigate this risk. Regularly review, evaluate, and update, if necessary, of the following IT controls:
 - a. Database administration practices.
 - b. Production control practices.

13. Users Awareness Training
Develop and update timely and relevant training material to raise the level of cybersecurity awareness of users throughout the organization.

ATTACHMENT B -- Data Use Agreement

AGREEMENT FOR CONFIDENTIAL DATA EXCHANGE BETWEEN SCHOOL DISTRICT AND CORE DISTRICTS

This Data Use and Confidentiality Agreement ("Data Use Agreement") between School District (as identified and signed in the joinder, Attachment E), and CORE Districts (referred to as CORE) with subcontractors Education Analytics (hereinafter referred to as EA), VersiFit Technologies LLC (hereinafter referred to as VFT), and Panorama Education (hereinafter referred to as PE), as well as with the CORE Research Partner at Policy Analysis for California Education (hereinafter referred to as PACE). Together, EA, VFT and PE are referred to as the "CORE Measurement Sub-Contractors" below. PACE is referred to as the "CORE Research Partner." This Data Use Agreement describes the means to be used by the CORE Measurement Sub-Contractors and CORE Research Partner to ensure the confidentiality and security and terms of use for information and data exchanged between School District, the CORE Measurement Sub-Contractors, and the CORE Research Partner for the purposes stated below. Within the scope of this agreement, confidential data may be exchanged between and amongst School District, the CORE Measurement Sub-Contractors, and the CORE Research Partner.

I. GENERAL TERMS

A. PURPOSE

The CORE Measurement Sub-Contractors have entered into service and measurement/analytical support partnerships with the CORE Districts (hereinafter, CORE). PACE¹ has a continued research support partnership with the CORE Districts. CORE is a non-profit organization comprised of member California school districts. The purpose of this Agreement is to assist School District, a member of the CORE Data Collaborative, to participate in measurement, analytics, reporting and research based upon CORE's school quality improvement indicator system. The CORE Measurement Sub-Contractors will collect and utilize longitudinal administrative data specific to the School Quality Improvement Index indicators and including related indicators in order to provide reporting to School District leaders and practitioners. Further, the CORE Research Partner will collect and archive longitudinal administrative data from the CORE data system to conduct policy analyses for School District leaders, School District practitioners and the public in order to support the continuous improvement in K-12 education. Public policy and other research questions to be addressed using the CORE Data Archive managed by our CORE

¹ Policy Analysis for California Education (PACE) is an independent, non-partisan research center based at Stanford University, in partnership with the University of Southern California and the University of California – Davis. Founded in 1983, PACE seeks to define and sustain a long-term strategy for comprehensive policy reform and continuous improvement in performance at all levels of California's education system, from early childhood to postsecondary education and training. PACE bridges the gap between research and policy, working with scholars from leading universities and research institutes in California and beyond and with state and local policymakers to increase the impact of academic research on educational policy in California. PACE works with a network of approximately 50 policy scholars from all of the leading research universities in California, both public and private.

Research Partner will be developed in collaboration with participating CORE Data Collaborative districts and representatives of CORE.

B. NATURE OF DATA

To further the achievement of the above stated purposes, School District will provide the CORE Measurement Sub-Contractors, and, in some cases, the CORE Research Partner with data extracts from the School District data systems to include data elements, Identified in Attachment C, necessary to produce and report the measures involved in CORE's school quality improvement data system, and to engage in meaningful analytics and research.

School District may also provide the CORE Measurement Sub-Contractors and/or CORE Research Partner with any additional items required to answer research questions defined by School District alone or with other CORE participants.

School District warrants that it has the authority to provide such data to the CORE Measurement Sub-Contractors and to the CORE Research Partner under the terms of this Agreement, and that School District will not be in breach of any law or representations to any person by providing such information to CORE Measurement Sub-Contractors and/or the CORE Research Partner.

These data extracts will include historical information wherever possible. Additional data elements may be provided at the discretion of School District.

The CORE Measurement Sub-Contractors and/or CORE Research Partner may collect data that contain confidential information, the disclosure of which is restricted by a provision of law. Some examples of "confidential information" include, but are not limited to, "personal information" about individuals as defined in California Civil Code Section 1798.3 of the Information Practices Act and "personal information" about students as defined by the Code of Federal Regulations CFR Title 34 Volume 1 Part 99.3.

C. TRANSFER OF DATA

School District and the CORE Measurement Sub-Contractors and CORE Research Partner shall use a secure electronic means and schedule for transferring confidential information. School District will create data extracts according to specifications provided by CORE. Extracts will be updated using a mutually agreed upon schedule (generally through annual submission the summer). Generally, data will be transferred by School District or their Partnering Education Agency to CORE's Measurement Sub-Contractors. For research and policy analysis purposes, such data or analyzed versions of such data may be transferred between and amongst CORE Sub-Contractors and CORE Research Partner as named in this Data Use Agreement; this agreement also covers the transfer of data from School District directly to the CORE Research Partner.

D. PERIOD OF AGREEMENT

This Agreement shall be effective from the signing of this agreement through June 30, 2020, unless terminated earlier by either party pursuant to Section F.

E. CORE DISTRICTS RESPONSIBILITIES

CORE agrees to the following confidentiality statements:

1. CORE acknowledges that these data are confidential data and proprietary to School District, and

agree to protect such information from unauthorized disclosures and comply with all applicable confidentiality laws which may include but is not limited to, the Health Insurance Portability and Accountability Act (HIPAA), the California Education Code and the Family Education Rights and Privacy Act (FERPA) as set forth in this agreement. The CORE Measurement Sub-Contractors and the CORE Research Partner are responsible for complying with all applicable District, Local, State and Federal confidentiality laws and regulations.

2. The CORE Measurement Sub-Contractors and CORE Research Partner will use appropriate safeguards to prevent the use or disclosure of the information other than as provided by this data use Agreement.
3. The CORE Measurement Sub-Contractors and CORE Research Partner shall (a) instruct all staff with access to confidential information about the requirements for handling confidential information (b) provide all staff with access to confidential information statements of organizational policies and procedures for the protection of human subjects and data confidentiality and (c) notify staff of the sanctions against unauthorized disclosure or use of confidential and private information. Other than as provided herein, no confidential data will be released by the CORE Measurement Sub-Contractors and CORE Research Partner.
4. The CORE Measurement Sub-Contractors and CORE Research Partner shall not assign this Agreement or any portion thereof to a third party without the prior written consent of School District, and any attempted assignment without such prior written consent in violation of this Section shall automatically terminate this Agreement. For clarification purposes, members of the PACE network who have signed a separate affiliated researcher agreement with PACE are not considered a third party.
5. The CORE Measurement Sub-Contractors and CORE Research Partner will use any information which could potentially allow the identification of any individual only for the purpose of creating the data sets using aggregate data and analyzing the data. The CORE Measurement Sub-Contractors and CORE Research Partner will not use or further disclose the information accessed or received other than as permitted by this Data Use Agreement or as otherwise required by law.
6. The CORE Measurement Sub-Contractors and CORE Research Partner will publically report only aggregate data and will not publicly report any individual data, nor will data be reported in a manner that permits indirect identification of any individual. At the direction of School District, the CORE Measurement Sub-Contractors and CORE Research Partner may provide School District leaders and practitioners secure, private access to School District student level data in alignment with School District's permission and security policies and procedures. This paragraph will survive the termination of this Agreement.
7. The CORE Measurement Sub-Contractors and CORE Research Partner will not contact the individuals included in the data sets without written consent from School District.
8. The CORE Measurement Sub-Contractors and CORE Research Partner agree to obtain written approval from School District prior to engaging any additional subcontractors or research partners to perform any services requiring access to any individually identifiable information. Notwithstanding the forgoing, the parties agree that CORE Research Partner may engage additional

members of the PACE network who have signed a separate affiliated researcher agreement with PACE to perform research services. PACE affiliated researchers will only utilize student data that is stripped of official state and district identifiers, and researchers will access data housed on a Stanford secure folder with restricted access.

9. The CORE Measurement Sub-Contractors and CORE Research Partner shall not re-disclose any individual-level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by School District.
10. The CORE Measurement Sub-Contractors and CORE Research Partner shall use the data only for the purpose stated above. These data shall not be used for personal gain or profit.
11. The CORE Measurement Sub-Contractors and CORE Research Partner shall keep all information furnished by School District in a space physically and electronically secure from unauthorized access. Information and data shall be stored and processed in a way that unauthorized persons cannot retrieve nor alter the information by means of a computer, remote terminal, or other means. No data will be stored unencrypted on laptop computers or other portable computing devices or media, e.g., flash drives, etc.
12. The CORE Measurement Sub-Contractors and CORE Research Partner shall permit examination and on-site inspections by School District upon reasonable advance notice for the purpose of ascertaining whether the terms of this Agreement are being met.

F. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL or FedEx):
 - a. By CORE or School District immediately in the event of a material breach of this Agreement by the other party.
 - b. By CORE or School District upon 30 days notice to the other party.
 - c. By CORE Research Partner or Measurement Subcontractors upon 30 days notices to CORE Districts.
2. Upon ninety (90) days written notice from School District, the CORE Measurement Sub-Contractors and CORE Research Partner shall delete all confidential and/or sensitive information promptly so that it is no longer accessible for analysis and exists only on a temporary back-up server that is encrypted. The CORE Measurement Sub-Contractors and CORE Research Partner shall also securely destroy all physical media (e.g., data on CDs or USB drives) containing confidential and/or sensitive information utilizing a mutually approved method of confidential destruction, which may include shredding, burning, or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. In the absence of such notice, the CORE Measurement Sub-Contractors and CORE Research Partner may continue to use such data for research, education or related purposes; or to meet CORE public reporting requirements.

G. PARTY LIABILITY; LIMITATION OF DAMAGES

1. The parties agree to defend, indemnify, and hold each other harmless from and against any loss, claim, or damage arising from the negligent acts or omission of their own officers, employees, students or agents in the performance of their duties under this Agreement.
2. EXCEPT FOR CLAIMS BASED ON WILLFUL MISCONDUCT, NEITHER PARTY, THEIR TRUSTEES, DIRECTORS, OFFICERS, EMPLOYEES, STUDENTS AND AFFILIATES SHALL BE LIABLE FOR PUNITIVE OR EXEMPLARY DAMAGES OF THE OTHER PARTY.

H. DISPUTES

In the event of a dispute among the parties to this Agreement regarding the provisions of this Agreement, any party may, by written notice to the other parties, call for mediation of the dispute before a mediator to be agreed upon by the parties. If the dispute is not resolved by mediation within 30 days of such notice, then any party may proceed to exercise all rights and remedies available under applicable law and this Agreement.

I. GENERAL UNDERSTANDING

1. This Agreement contains the entire understanding of the parties and may only be amended in writing signed by the parties. This Agreement may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to be one and the same document. The parties may sign and deliver this Agreement by facsimile or using other electronic means (including digital signatures). Copies of this Agreement shall be treated as originals.
2. This Agreement constitutes the full and complete agreement between the parties, and supersedes all prior written and oral agreements, commitments or understandings with respect thereto.
3. This Agreement shall be governed by and construed under the laws of the State of California. Venue for any proceeding relating to enforcement of this Agreement shall be in the California state courts located in Sacramento County, California.
4. Any waiver by a party of a violation of any provision of this Agreement shall not bar any action for subsequent violations of the Agreement.

J. Signatures

Signed:
CORE DISTRICTS



Rick Miller, Executive Director

May 17, 2016

Date

PACE
Board of Trustees of the Leland Stanford
Junior University

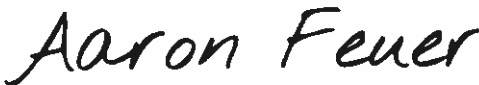


Nicole Pobuta | Contract & Grant Officer
May 13, 2016

May 13, 2016

Date

PANORAMA EDUCATION



Aaron Feuer, CEO

05 / 16 / 2016

Date

EDUCATION ANALYTICS



Andrew Rico, VP Research & Operations

5/13/16

Date

VERSANT TECHNOLOGIES



Jonathan Bissenbach, COO

5-16-2016

Date

**ATTACHMENT C:
SPECIFIC DATA ELEMENTS REPORTS THAT MAY BE INCLUDED IN THE CORE DATA COLLABORATIVE**

Attachment C - SPECIFIC DATA ELEMENTS THAT MAY BE INCLUDED IN THE CORE DATA COLLABORATIVE (UPDATED 5.12.16)		
Data Element(s) Applies to all students in grades K-12 unless noted otherwise	Variables to include (Subject to Adjustment)	Additional Notes
Standardized Tests (student level data)		
SBAC Summatives all grades (3-11) & Subjects (ELA & Math)	Student ID, CDS code (14 digits), grade level, subject, sub-subject/sub-component (if available), score, performance band, etc.	Key Indicator
SBAC and/or other interim/benchmark assessments	Student ID, CDS code (14 digits), grade level, subject, sub-subject/sub-component (if available), score, performance band, etc.	Additional Indicator
CELDI information	Student ID, CDS code (14 digits), grade level, subject, sub-subject/sub-component (if available), score, performance band, etc.	Key/Additional Indicator
Other standardized test results (e.g., AP, IB, SAT, ACT)	Student ID, CDS code (14 digits), grade level, subject, sub-subject/sub-component (if available), score, performance band, etc.	Additional Indicator
Student Characteristics (student level data)		
Student demographics	Student district ID, Student state ID, gender, grade level, race/ethnicity, free/reduced lunch status, mother education attainment, father education attainment, first U.S. school entry date	Key Indicator
District entry date	Student ID, district entry date	Key Indicator
Special Education flag	Student ID, special education flag (Yes or no)	Key Indicator
English Language information	Student ID, EL status (EL or RFP), date identified as EL, date reclassified as RFP	Key Indicator
Foster care flag	Student ID, foster care flag (yes or no)	Key Indicator

Attachment C - SPECIFIC DATA ELEMENTS THAT MAY BE INCLUDED IN THE CORE DATA COLLABORATIVE (UPDATED 5.12.16)		Additional Notes
Data Element(s)	Variables to Include (Subject to Adjustment)	
Enrollment, Attendance and Discipline [student level data; for each school of attendance]		
Days enrolled	Student ID, CDS code (14 digits), total days enrolled	Key Indicator
Days present (alternative: Days absent)	Student ID, CDS code (14 digits), total days present (alternative: total days absent)	Key Indicator
School entry and leave date	Student ID, CDS code (14 digits), entry date, leave date	Key Indicator
Total number of out of school suspensions (alternatively, each suspension per student is listed in a separate row)	Student ID, CDS code (14 digits), suspension count	Key Indicator
Expulsion flag	Student ID, CDS code (14 digits), expulsion flag (yes or no)	Key Indicator
Course Information, Graduation Information, Program Information and Staff Information		
Course information	Student ID, CDS code (14 digits), semester (e.g., fall or spring), department (subject area), name of course, Calpad course code, district course code, credits earned, course marks, flag for required 8th grade courses, potentially flags for other course identifiers (e.g., AP, IB, concurrent enrollment, career pathway information), and teacher-student-course linkage information	Key/additional indicator
Staff information	Role, years of experience, demographics (race/ethnicity, gender), education/certification, staff ID	Additional Indicator
Program information	Program participation, program dosage, program performance	Additional Indicator
Unweighted end of the year GPA (based only on fall and spring semesters) for 6th to 12th grades	Student ID, CDS code (14 digits), unweighted end of year GPA	Key/additional indicator
High school graduation flag	Student ID, CDS code (14 digits), graduation indicator	Additional Indicator
Students in graduation cohort	Student ID, CDS code (14 digits), cohort year	Additional Indicator

Attachment C - SPECIFIC DATA ELEMENTS THAT MAY BE INCLUDED IN THE CORE DATA COLLABORATIVE (UPDATED 5.12.16)

Data Element(s) Applies to all students in grades K-12 unless noted otherwise	Variables to include (Subject to Adjustment)	Additional Notes
School Information	School name, CDS code (14 digits), district code, grades served, school level, SIG status and year, charter status, type of school (credit recovery programs, independent study schools, schools for students with severe disabilities, schools for expelled students, and early childhood education programs)	
School level data		
College Going Information	Examples include college application data, college persistence data, college completion data	Additional Indicator
College going data		

Attachment E

Joinder Agreement – San Pasqual Union School District and CORE Districts Data Use Agreement

This Joinder Agreement (hereinafter referred to as “Joinder”) is effective as of July 1st, 2019 by and among the undersigned San Pasqual Union School District (hereinafter referred to as SPUSD), whose address is listed on the signature page hereto, and the parties to that certain Data Use and Confidentiality Agreement dated May 2016 (“the Data Use Agreement”)

SPUSD hereby agrees that upon execution of this Joinder, SPUSD shall be bound by all of the terms and conditions of the Data Use Agreement and shall be deemed a party to such Data Use Agreement in all respects.

This Joinder, together with the Data Use Agreement, represents the entire agreement and understanding between the parties with respect to its subject matter. The Joinder, together with the Data Use Agreement, supersedes all prior or contemporaneous discussions, representations, or agreement, whether written or oral, of the parties regarding this subject matter.

As the data in this Data Use Agreement is part of a collective project for the San Diego County Superintendent of Schools, data will be collected and organized first by the San Diego County Superintendent of Schools and then provided to the parties named in the Data Use Agreement.

San Pasqual Union School District
15305 Rockwood Road
Escondido, CA 92027

Signature: _____

Name: _____

Title: _____

Address: _____

Phone: _____

Email: _____