

**Data Sharing Agreement Between
Gateway Community Charters
and
Innovate for California**

This Data Sharing Agreement ("Agreement") is entered into as of 17th of July, 2024, by and between Gateway Community Charters ("District"), Innovate for California ("Consultant"). District, Vendor and Consultant may each be referred to as "Party" or together as the "Parties" in this Agreement.

RECITALS

- A. **WHEREAS**, Consultant wishes to access certain student data and related information collected or maintained by District ("District Data") for the purpose of providing data to and for the District, the District's authorizing agents and for non-PI and non-PII aggregate publicly display.
- B. **WHEREAS**, Consultant is willing to undertake the project and utilize the District Data in strict accordance with all applicable laws and regulations governing student data privacy, and is further willing to share results of the Study with the District at no charge; and
- C. **WHEREAS**, the District, in acknowledging that the results of the project may benefit District students by improving instruction and student achievement, is willing to share certain District Data specified hereunder with Consultant; and
- D. **WHEREAS**, the Parties now desire to enter into this Agreement setting forth the terms and conditions pursuant to which the District will share certain District Data with Consultant, subject to the terms and conditions set forth herein.

AGREEMENT

NOW, THEREFORE, the Parties agree as follows:

- 1. Purpose. The purpose of this Agreement is to set forth the terms and conditions pursuant to which the District will grant Consultant access to certain District Data as identified hereunder, for the sole purpose of permitting Consultant to conduct the Study, in compliance with all applicable state and federal laws, regulations, and District policies governing student data privacy.
- 2. Applicable Law. The Parties agree that all processing, storing, transfer, transmittal, sharing and use of District Data under this Agreement shall comply with the requirements for maintaining the privacy of student records including, but not limited to Education Code section 49060 *et seq.*, the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99, as amended), District policies regarding the protection and confidentiality of District Data, and other state and federal laws and regulations regarding educational records, student data privacy, and confidentiality ("Law"), and further agree to

prevents the interception, diversion, or other unauthorized access to said District Data.

- ii. Ensure that access to District Data is limited to personnel who are authorized to have such access under this Agreement.
 - iii. Ensure that access to any PII included in the District Data shall be restricted to those individuals with a legitimate educational interest and need for access in order to carry out the purposes set forth above in this Agreement, as set forth in Law.
 - d. The confidentiality requirements under this Section shall survive the termination or expiration of this Agreement or any subsequent agreement intended to supersede this Agreement.
5. Data Breach Procedures. Should Consultant inadvertently disclose PI, PII and/or other District Data to any third party, Consultant will promptly notify the District, in no event more than two (2) business days, after Consultant becomes aware of any suspected or actual breach or incident. The District will promptly investigate the incident and will take any corrective action necessary to remedy any breach or security incident, which remedies may include termination of this Agreement. Consultant further agrees to immediately return or destroy any retained copies of District Data at the District's request.
6. Media or Public Statements. Consultant agrees not to make any media or public statements about the Study, including the fact that the Study is taking place, without the express written consent of the District. Consultant further agrees not to release or publish any articles, reports, papers, or other publications derived from District Data disclosed to Consultant as part of this Agreement without the express written consent of the District.
7. Indemnity. Each Party agrees to defend, indemnify, and hold harmless the other Party, its officers, employees, agents, governing board, and members of its governing board, harmless from and against any liability, loss, expense (including attorneys' fees), or claims of injury or damages arising out of the indemnifying Party's performance of the terms of this Agreement, including but not limited to claims arising from or related to the inadvertent or unauthorized disclosure of District Data, but only in proportion to and to the extent such liability, loss, expense, attorney's fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the indemnifying Party, and/or its officers, employees, or agents.
8. Insurance. Without limitation of any indemnification obligations set forth in this Agreement, each Party shall be self-insured or maintain an insurance policy with sufficient coverage and limits to cover claims arising out of or related to this Agreement. Each Party shall provide documentation to the other Party verifying such coverage and limits upon written request.

prevents the interception, diversion, or other unauthorized access to said District Data.

- ii. Ensure that access to District Data is limited to personnel who are authorized to have such access under this Agreement.
 - iii. Ensure that access to any PII included in the District Data shall be restricted to those individuals with a legitimate educational interest and need for access in order to carry out the purposes set forth above in this Agreement, as set forth in Law.
 - d. The confidentiality requirements under this Section shall survive the termination or expiration of this Agreement or any subsequent agreement intended to supersede this Agreement.
5. Data Breach Procedures. Should Consultant inadvertently disclose PI, PII and/or other District Data to any third party, Consultant will promptly notify the District, in no event more than two (2) business days, after Consultant becomes aware of any suspected or actual breach or incident. The District will promptly investigate the incident and will take any corrective action necessary to remedy any breach or security incident, which remedies may include termination of this Agreement. Consultant further agrees to immediately return or destroy any retained copies of District Data at the District's request.
 6. Media or Public Statements. Consultant agrees not to make any media or public statements about the Study, including the fact that the Study is taking place, without the express written consent of the District. Consultant further agrees not to release or publish any articles, reports, papers, or other publications derived from District Data disclosed to Consultant as part of this Agreement without the express written consent of the District.
 7. Indemnity. Each Party agrees to defend, indemnify, and hold harmless the other Party, its officers, employees, agents, governing board, and members of its governing board, harmless from and against any liability, loss, expense (including attorneys' fees), or claims of injury or damages arising out of the indemnifying Party's performance of the terms of this Agreement, including but not limited to claims arising from or related to the inadvertent or unauthorized disclosure of District Data, but only in proportion to and to the extent such liability, loss, expense, attorney's fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the indemnifying Party, and/or its officers, employees, or agents.
 8. Insurance. Without limitation of any indemnification obligations set forth in this Agreement, each Party shall be self-insured or maintain an insurance policy with sufficient coverage and limits to cover claims arising out of or related to this Agreement. Each Party shall provide documentation to the other Party verifying such coverage and limits upon written request.

9. Destruction or Return of District Data. All District Data received by Consultant under this Agreement shall be destroyed or returned to District when it is no longer needed for the Study and no later than 5 years after the District Data is first received.

10. Term; Termination.

- a. This Agreement will terminate in 365 days after the agreement has been signed unless earlier terminated as provided herein, or renewed in writing by the Parties.
- b. This Agreement may be terminated by either Party at any time, for any reason, by written notice to the other Party. At the time of termination, Consultant will return any District Data to District or destroy the same, as requested by District.

11. Notices. Any notice, demand, approval, consent, or other communication between the Parties will be provided to the following addressees:

To District:

Gateway Community Charters.

Address: 5112 Arnold Ave Suite A, McClellan Park, CA 95652

Attention: Adam VeVea & Matt Taylor

Email: matt.taylor@gcccharters.org & adam.vevea@gcccharters.org

To Consultant:

Shawn Dean (Innovate for California)

Address: 7408 Pratte Ave, CA 95621

Attention: Shawn Dean

Email: shawnshawn@innovateforcalifornia.com

Notice may be provided by personal service, regular mail, certified mail, overnight mail with proof of delivery, facsimile with proof of transmission, or by email provided receipt is acknowledged. By writing notice to the other, either Party may change its mailing address or correspondence information.

12. No Partnership. Consultant and District are not partners and nothing herein contained shall be construed to create a partnership or joint venture in any sense.

13. No Assignment. Neither Party shall assign its rights or privileges under this Agreement, or any interest therein, and shall not attempt to confer any of its privileges under this Agreement to any third party.

14. Amendments. This Agreement may be modified or amended only with the written consent of both Parties.

15. Governing Law; Venue. This Agreement shall be governed by and interpreted under the laws of the State of California applicable to instruments, persons, transactions and subject matter which have legal contacts and relationships exclusively within the State of

California. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the Superior Court of the State of California for Sacramento County, subject to any transfer of venue as required by law.

16. Entire Agreement. This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof, and no prior agreement, statement, promise, or representation made by any party, employee, officer, or agent which is not contained herein shall be binding or valid.
17. Execution in Counterparts. This Agreement may be executed in counterparts such that the signatures may appear on separate pages. A copy, or an original, with all signatures appended together shall be deemed a fully executed agreement. Signatures transmitted by facsimile shall be deemed original signatures.
18. Warrant of Authority. Each of the persons signing this Agreement represents and warrants that such person has been duly authorized to sign this Agreement on behalf of the Party indicated, and each of the Parties by signing this Agreement warrants and represents that such Party is legally authorized and entitled to enter into this Agreement

EXHIBIT "A"
SCHEDULE OF DATA

Category of Data	Elements & Purpose	Check if Used by Your System
Application Technology MetaData	To comply with California Education Code (e.g., § 49073.1) we are required to log the IP Addresses of any users and their use of cookies.	X
	Other application technology metadata-Please specify:	
Application Use Statistics Assessment	To comply with California Education Code (e.g., § 49073.1)we are required to track Metadata on user interaction with applications.	X
	Standardized test scores to do correlation studies (comparing standardized test scores to student achievement, student outcome and other assessments)	X
	Other assessment data-Please specify: I-ready csv reports	X
Attendance	Student school (daily & monthly) attendance data	X
	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	
Conduct	Aeries Intervention Management System	X
Demographics	Date of Birth	
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify: To validate our data we compare our results to Aeries Student Extended Fields.	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X

	Guidance counselor	
	De-Identified Guidance Counselors ID #	X
	Specific curriculum programs	X
	Year of graduation (cohort-year)	X
	Other enrollment information-Please specify: Enrollment/Attendance History	X
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	De-Identified Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	X
	Teacher names	
	De-Identified Teacher Id Number	X
Special Indicator	English language learner information	X
	Low income status	X
	Vision / hearing test results	X
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	X
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	

	Phone	
Student Identifiers	Local (School district) ID number (Aeries Student ID number & Aeries' Student Number)	X
	State ID number	
	3rd party vendor student identifications number (created to link student to 3rd party applications)	X
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify:	
Transcript	Student course grades	X
	Student course data	X
	Student course grades/ performance scores	X

Category of Data	Elements	Check if Used by Your System
	Transcript Data	X
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	

Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "B" **DEFINITIONS**

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Aggregate Data: Aggregate Data is defined as a group of people that are no less than 10.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept 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.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect

to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Anonymized or de-identified, or anonymous data will be collected as stated in **Exhibit "A"**. Until such time Student Data has been stripped of all personally identifiable information (PII), Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Personally Identifiable Information: Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

[SIGNATURES BELOW]

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: Gateway Community Charters

By: Adam VeVea Date 7/17/24

Printed Name: Adam VeVea Title Dir. of Data & Accountability

By: [Signature] Date 7/17/24

Printed Name: Matt Taylor Title Chief of Staff

Provider: Innovate For California

By: [Signature] Date 7/17/24

Printed Name: Shawn Dean Title President