

**STANDARD STUDENT DATA PRIVACY  
AGREEMENT**

**CA-NDPA Standard**  
Version 1.0 (10.22.20)

Education Technology Joint Powers Authority

and

Panorama Education, Inc.

September 15, 2021

This Student Data Privacy Agreement ("DPA") is entered into on September 15, 2021 (the "Effective Date") and is entered into by and between:

Education Technology Joint Powers Authority, located at 5050 Barranca Parkway, Irvine, CA 92604 (the "Local Education Agency" or "LEA") and Panorama Education, Inc., located at 24 School Street, 4th Floor, Boston, MA 02108 (the "Provider").

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99), the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), and applicable state privacy laws and regulations

and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the SDPC Standard Clauses hereto.

**2. Special Provisions. Check if Required**

If checked, the Supplemental SDPC State Terms attached hereto as **Exhibit "G"** are hereby

incorporated by reference into this DPA in their entirety, as agreed upon by the parties.

If Checked, the Provider, has signed **Exhibit "E"** to the SDPC Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of an express conflict between the SDPC Standard Clauses and the Special Provisions, the latter will control. In the event there is an express conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider's terms of service or privacy statement, the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. Exhibit E will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "Services").
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

---

The designated representative for the LEA for this DPA is:

Name: Diana Lav Title: Account Executive

Address: 24 School Street, 4<sup>th</sup> Floor, Boston, MA 02108

Phone: (617) 925 5749 Email: dlav@panoramaed.com

The designated representative for the Provider for this DPA is:

Name: Michelle Bennett Title: Procurement Specialist

Address: 5050 Barranca Parkway, Irvine, CA 92604

Phone: 949-936-5022 Email: MichelleBennett@iusd.org

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

**LEA: Education Technology Joint Powers Authority**

By:  Date: 9/3/21

Printed Name: Brianne Ford Title/Position: President

**PROVIDER: Panorama Education, Inc.**

By:  Date: 09/02/2021

Printed Name: Katie Mallett Title/Position: COO

## **STANDARD CLAUSES**

Version 3.0

### **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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. For purposes of FERPA, in performing services pursuant to the Service Agreement, the Provider shall be considered a School Official with a legitimate educational interest, and performing institutional services or functions otherwise provided by the LEA's employees. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.
2. **Student Data to Be Provided.** In order for Provider to perform the Services described in Exhibit "A", LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of an express conflict, definitions used in this DPA shall prevail over definitions used in any other writing, including, but not limited to the Service Agreement or Provider's privacy statement.

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, in performing Services pursuant to the Service Agreement, the Provider shall be considered a School Official with a legitimate educational interest, performing institutional services or functions otherwise provided by the LEA's employees, and under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Educational Records and/or Student Data and/or correct erroneous information, and reasonable procedures for the transfer of Student-Generated Content to a personal account, consistent with the functionality of the Services. Provider shall respond in a reasonably timely manner, but in no event more than forty-five (45) days, after a written request by LEA, or pursuant to the time frame required under state law, that enables an LEA to timely respond to a request by parent, legal guardian or eligible student to view or correct their Student Data to the extent held by the Provider. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall,

at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student Generated Content to a separate account created by the student, consistent with the functionality of the Services.

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Educational Records and/or Student Data under FERPA {34 CFR § 99.31{a}{l}}, LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and Student Data hosted by Provider or Subcontractor hired by Provider.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security to the extent applicable to Provider's performance of Services, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A and/or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or Personally Identifiable Information contained in the Student Data other than as directed or permitted in writing by the LEA or this DPA. This prohibition against re-disclosure shall not apply to aggregate summaries of De-Identified Data, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or Student Data disclosed to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-identified Student Data. De-Identified Data may be used and disclosed by the Provider for those purposes allowed under FERPA, applicable state laws, the Services Agreement, and the following purposes:
  - (1) assisting the LEA or other governmental agencies in conducting research and other studies; and
  - (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer De Identified Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. For the avoidance of doubt, the transfer restriction shall not be construed as prohibiting re-disclosure of Student Data or De-Identified Data otherwise contemplated in this DPA. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II, section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Provider's servers that store Student Data shall be located within the United States. Provider shall not knowingly store Student Data on Subprocessors' servers located outside of the United States. Upon written request of the LEA, Provider will provide a list of the locations where Student Data is stored on Provider's and/or Provider's subprocessors' servers.

2. **Audits.** No more than once a year, or following a breach under to Article V, Section 4, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the Provider's delivery of Services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and records pertaining to the Provider's delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to reasonably protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security to the extent applicable to Provider's performance of Services for LEA. The Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in Exhibit "F". Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to Exhibit "F". Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in Exhibit "F". Provider shall provide, in the Standard Schedule to the DPA, Provider's contact information that LEA may use if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider ("Breach"), the Provider shall provide notification to LEA most expedient time possible of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made as required under applicable law within a reasonable time after the incident and when law enforcement allows notification. Provider shall follow the following process:
  - (1) The incident notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a Breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the Breach, (2) the estimated date of the Breach, or (3) the date range within which the Breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the Breach incident, if that information is possible to determine at the time the notice is provided.
    - vi. The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.
  - (2) Provider agrees to adhere to all federal and state requirements to the extent applicable to Provider with respect to a data breach (as defined under applicable law) related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and applicable 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, including Personally Identifiable Information, and agrees to provide LEA,



upon written request, with a summary of said written incident response plan.

- (4) If and as required under applicable law and/or LEA's policy, LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. The duty to return or destroy data in accordance with Article IV, section 6, above shall survive the termination, as will the other terms of this DPA, until the return of the destruction of the data is accomplished. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall dispose all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is express conflict between the terms of the DPA and the Service Agreement, or Provider's privacy statement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the Standard Clauses and the Special Provisions, the latter will prevail. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

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 THE LEA, WITHOUT 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 THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
  
7. **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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA in a reasonably timely manner. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
  
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

**[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.  
IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST EACH PRODUCT  
(RESOURCE) HERE]**

**Social and Emotional Learning Assessment System**

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input checked="" type="checkbox"/>
	Other application technology meta data- Please specify: <b>operating system, browser version, device type, location (from IP address)</b>	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input checked="" type="checkbox"/>
	Observation data	<input checked="" type="checkbox"/>
	Other assessment data-Please specify: <b>See Note 1 below.</b>	<input checked="" type="checkbox"/>
Attendance	Student school (daily) attendance data	<input checked="" type="checkbox"/>
	Student class attendance data	<input checked="" type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input checked="" type="checkbox"/>
Demographics	Date of Birth	<input checked="" type="checkbox"/>
	Place of Birth	<input checked="" type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>
	Ethnicity or race	<input checked="" type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input checked="" type="checkbox"/>
	Other demographic information-Please specify: <b>See Note 1 below.</b>	<input checked="" type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input checked="" type="checkbox"/>
	Guidance counselor	<input checked="" type="checkbox"/>
	Specific curriculum programs	<input checked="" type="checkbox"/>
	Year of graduation	<input checked="" type="checkbox"/>
	Other enrollment information-Please specify: <b>See Note 1 below.</b>	<input checked="" type="checkbox"/>
Parent/Guardian Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System	
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Parent / Guardian Name	First and/or Last	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schedule	Student scheduled courses	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special Indicator	English language learner information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Low income status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Medical alerts/ health data	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student disability information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other indicator information-Please specify: <b>See Note 1 below.</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Contact Information	Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>	<input type="checkbox"/>

	Other student work data -Please specify:		
Transcript	Student course grades		√
	Student course data		√
	Student course grades/ performance scores		√

Category of Data	Elements	Check if Used by YOUR System
	Other transcript data - Please specify: <b>See Note 1 below.</b>	√
Transportation	Student bus assignment	√
	Student pick up and/or drop off location	√
	Student bus card ID number	√
	Other transportation data - Please specify: <b>See Note 1 below.</b>	√
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p><b>Note 1: Data that Provider may request or require as part of providing Services is indicated in this Exhibit B. Each LEA ultimately determines the data it makes available as part of Provider's Services, and it may choose to send to Provider data not explicitly listed in Exhibit B, covered by various "Other" categories. Such data is impossible to exhaustively list, because each LEA determines the data relevant to its purpose and objectives with Provider. Provider expects each LEA to choose the subset of the data in Exhibit B to use in conjunction with Provider's Services and to provide only the information necessary for LEA's objectives and purposes.</b></p>	

None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable .	<input type="checkbox"/>
------	--	--------------------------



## EXHIBIT "C"

### 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.

**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 definition.

**Originating LEA:** A local education agency who executes the original 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, but it does not include student responses to a standardized assessment where student possession and control would undermine or compromise the validity and reliability of that assessment.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31 (a)(1)(i)(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 Educational 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 and/or terms of service and/or terms of use between Provider and LEA for the Services.

**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,

I 190353v1

identifying Information contained 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 that has not been stripped of direct and indirect identifiers. 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. Student Data shall constitute Educational Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's Services shall not constitute Student Data if used in a manner allowed by this DPA.

**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 Services, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original DPA 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" as used in some state statutes means a provider of digital educational software or services, including cloud based services, for the digital storage, management, and retrieval of Student Data. Within this DPA, the term "Third Party" is replaced by the term "Provider."

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

Provider to dispose of data obtained by Provider  
pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable. By

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

**EXHIBIT "E"**  
**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Education Technology Joint Powers Authority ("Originating LEA") which is dated September 15, 2021, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

Kmallett@panoramaed.com

PROVIDER: Panorama Education

BY: Katie Mallett Date: 9/2/2021

Printed Name: Katie Mallett Title/Position: COO

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Subscribing LEA

and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS. SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VI \*\***

LEA: \_\_\_\_\_

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

**DESIGNATED REPRESENTATIVE OF LEA:**

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_

Email: \_\_\_\_\_

1190353v1

**EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by Provider.

**Cybersecurity Frameworks**

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
✓	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology - Security techniques - Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)

<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.eds.pex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

1190353v1

**EXHIBIT "G"**  
**Supplemental SDPC State Terms for California**  
**Version 1.0**

This Amendment for SDPC State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between: Education Technology Joint Powers Authority, located at 5050 Barranca Parkway, Irvine, CA 92604 (the "**Local Education Agency**" or "**LEA**") and Panorama Education, Inc., located at 24 School Street, 4th Floor, Boston, MA 02108 (the "**Provider**"). All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

**WHEREAS**, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws; and

**WHEREAS**, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584; California Assembly Bill 1584 ("**AB 1584**") at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

**WHEREAS**, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable California state laws and regulations.

**NOW, THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

**Term.** The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.

**Modification to Article IV, Section 7 of the DPA.** Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data ~~(i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; and (iii) to notify; or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify teacher account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.~~ account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

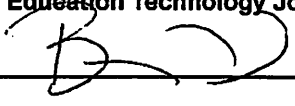
**(SIGNATURES BELOW)**

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

Date.

---

**LEA: Education Technology Joint Powers Authority**

By: 

Date: 9/3/21

Printed Name: Brianne Ford Title/Position: President

**PROVIDER: Panorama Education, Inc.**

By: 

Date: 09/02/2021

Printed Name: Katie Mallett Title/Position: COO

830-5/6173630.1