

**STANDARD STUDENT DATA PRIVACY AGREEMENT**

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

Education Technology Joint Powers Authority  
and

Instructure, Inc.

February 7, 2022

This Student Data Privacy Agreement ("DPA") is entered into on February 7, 2022 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 Instructure, Inc., located at

6330 S 3000 E, Ste. 700, Salt Lake City, UT 84121

(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), 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 Standard Clauses hereto.

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

X

If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

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

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for five (5) years. Exhibit E will expire five (5) 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:

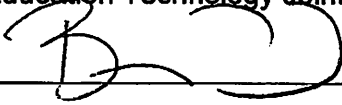
Name: Michelle Bennett Title: Procurement Specialist  
Address: 5050 Barranca Parkway, Irvine, CA 92604  
Phone: 949-936-5022 Email: MichelleBennett@iusd.org

The designated representative for the Provider for this DPA is:

Name: Daisy Bennett Title: Privacy Officer  
Address: 6330 S 3000 E, Ste. 700, Salt Lake City, UT 84121  
Phone: 800-203-6755 Email: privacy@instructure.com

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

LEA: Education Technology Joint Powers Authority

By:  Date: 2/16/22  
Printed Name: Brianne Ford Title/Position: President

**PROVIDER:**

By: Daisy Bennett Date: 02.07.2022  
Printed Name: Daisy Bennett Title/Position: Privacy Officer

## **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. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. 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 to perform the Services described above, 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 a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### **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, the Provider shall be considered a School Official, 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 Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. 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.

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 Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), 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 hosted Student Data.
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 applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, 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 disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or 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 by the Provider for those purposes allowed under FERPA 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 Student 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. 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, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, 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 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 all records pertaining to the Provider, LEA and 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 protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. 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, contact information of an employee who LEA may contact 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 the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation 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 within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach 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.
  
  - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach 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 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 request, with a summary of said written incident response plan.

- (4) 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. 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 destroy 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 conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, 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 Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. 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 no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. 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.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**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]**

**Learning Management Solution, Assessment Solution, Educational Intelligence and Analytics Solution.**

**Canvas Learning Management System  
Canvas Studio  
Mastery Connect**

Attached list of Instructure Products

Elevate Data Sync

Elevate Data Quality

Mastery View Assessments (Predictive & Formative)

Mastery View College Prep Assessment

Mastery Item Banks

Elevate K-12 Analytics

Elevate Data Sync

Elevate Standards Alignment

Elevate Data Quality

## Instructure Products

### Mastery View Assessments

#### Mastery View Predictive Assessments

Feature	Description
Online administration and scoring	Assessments are administered and scored online using the Mastery Connect assessment management system.
Customization to scope and sequence	Districts have the option to customize the standards assessed on each Mastery View Predictive Assessments to match their district's common scope and sequence (where available).
Mastery Pacing Guides	The Mastery Pacing Guides provide a state-specific suggested scope and sequence for assessments.
Predictive report	The Predictive Reports indicate each student's expected score on the state assessment score following each assessment administration window.
Standard and blueprint alignment	Rigorous alignment ensures that students are assessed on multiple key state-specific learning standards and closely match the state assessment blueprint.

Feature	Description
Final comprehensive	The Final Comprehensive Assessment is given towards the end of a course, covering all standards for that course.
Tools & accommodations	A variety of tools and accommodations, including text-to-speech and paper-pencil administration, can be utilized for students who need additional assessment support.

## Mastery View Formative Assessments

Feature	Description
Online administration and scoring	These prebuilt, expert-developed assessments are administered and scored online using Mastery Connect assessment management system.
Standards alignment	Each collection of ELA and Math assessments are closely aligned to essential standards of each state (availability varies by state and subject)
Single-standard and passage-based assessments	Each math assessment is single standard aligned; ELA assessments may be aligned to 1-3 standards per assessment.
Short-form	Each assessment has no more than 10 items and is meant to take no more than one class period to administer.
DCM scoring	The Diagnostic Classification Model is a proprietary psychometric model which allows fewer test questions while maintaining the high levels of reliability and validity.



## Mastery View College Prep Assessment

Feature	Description
Paper-and-pencil delivery	The Mastery View College Prep Assessment is administered in a paper-pencil format.
ACT Prep	The Mastery View College Prep Assessment is designed to prepare students to take the ACT Assessment.
Quick, predictive results	Results are returned within 72 hours of the test administration; results are shown to accurately predict performance on the ACT test.
Diagnostic data	Data is diagnostic in nature, allowing educators and students to pinpoint areas in need of improvement prior to the ACT Assessment.
Multiple data points	Multiple data points are reported across each subject area.



## Mastery Item Banks

### Mastery Item Bank and Mastery Item Bank Supplemental

Feature	Description
Standards alignment	Each of the 98,000+ high-quality, vetted items are carefully aligned to state standards; coverage in each state varies by subject and number of items. Mastery Item Bank is available in all fifty states and DC; Mastery Item Bank Supplemental is available in select states.
Technology-enhanced items	Tech-enhanced items, similar to those found on end-of-level state tests, are those in which students interact with the item (ie Drag and Drop, Highlight, etc), rather than simply selecting the correct answer in a multiple-choice format.
Filtering	Filtering allows items to be quickly discovered by subject, grade, class/course, and standard; items can be filtered by language, print capability, multi-part, passage inclusion, etc.
Passage items	Passages are any text, picture, video, etc. that are aligned to more than one item; users can filter by passage to see all associated items aligned to the passage.
Spanish-translated & transadapted items	Items may be translated and/or trans-adapted from English items to Spanish items or may be unique Spanish content.
DOK & difficulty information	Metadata for Depth of Knowledge (DOK) and difficulty level are included with each item.



Feature	Description
Auto and rubric scoring	Items are either auto-scored or rubric-scored; assessments with auto-scored items will provide a score immediately when the assessment is submitted. Rubric-scored items will be available for teachers to evaluate and score based upon the provided rubric.
Multi-step item development/review process	Items go through an intensive development and review process; all items are developed by content specialists and then thoroughly reviewed through a five-step review process to ensure validity and reliability.



# Elevate

## Elevate K-12 Analytics

Feature	Description
Hosted operational data store based on Ed-Fi standards	Underpinning Elevate K-12 Analytics is an operational data store which provides interoperability across systems and stores three years of educational data.
Analytics Visuals	Visuals allow select users to view the charts and dashboards in the Visuals Library. Users can also view visuals shared by their organization and may be able to create a new dashboard.
Analytics Watchlists	Watchlists allow users to track and easily view key metrics for selected groups of students. Watchlists also display links to view individual student information, including their Scorecard.
Analytics Perspectives	Perspectives present information in interactive data widgets that allow observation and tracking of various activities against organizational goals.
Data Explorer	The Data Explorer allows users to dissect information in various ways to better understand the underlying components of data. The Data Explorer initially displays aggregated data for a specified metric. Users can then interact with the data, filtering and disaggregating it so that users can compare, contrast, and apply investigative techniques to make inferences, observe statistical trends, and identify relationships between data.





Feature	Description
Student Scorecard	<p>Elevate K-12 Analytics student scorecards display overall student data and progress toward metric key performance indicators (KPIs) set by your institution. However, the charts displayed in a scorecard are dynamic.</p> <p>Use the Scorecard sidebar to manage the scorecard or further analyze student data or metrics using the Data Explorer.</p>

## Elevate Standards Alignment

Feature	Description
Academic Benchmarks repository of standards	The Academic Benchmarks repository contains over seven million machine-readable learning standards; each learning standard is reflective of a robust data model with up to 150 metadata fields. Standards are organized within a hierarchy of data which includes an authority or authoring governing body (i.e. Texas Education Agency), publication (i.e. Texas Essential Knowledge and Skills), document (i.e. English Language Arts and Reading, 2017).
Standards alignment API	The Elevate Standards Alignment (AB Connect) API helps developers and product managers integrate standard data and content alignments into systems, improving discoverability and accuracy.
Derivatives	A derivative standard relationship is created when a state has adopted a set of standards that were derived from another publication, typically from a National authority (i.e. Common Core State Standards). Derivative relationships are defined through data analysis and not limited to political affiliations.
Crosswalks	Curated Crosswalks create relationships among standards created by subject matter experts and share one or more skills; crosswalks enable



Feature	Description
	comprehensive views and comparisons. Crosswalks expedite and maintain alignment of content to multiple states and market segments.
AB GUIDs	The AB GUID (globally unique identifier assigning) is intelligent metadata that is assigned to every element in the database, promoting interoperability.
AB taxonomies	Taxonomic metadata includes topics and concepts, which are organized into key ideas, providing a common vocabulary for describing and tagging learning objects, including assessment content, instructional lessons, supplemental materials, and descriptive skills and objectives.
Client taxonomies	In addition to in-house developed taxonomies, client taxonomies can be supported as an intermediary for both content tagging as well as standards tagging.
Standards browser	The Standards Browser supports an intuitive browsing experience, leveraging the AB Connect API and features example widgets for use within products.
Standards search and alignment	Leveraging Elasticsearch, the AB Connect API supports robust standards searching and content alignment solutions; AP calls enable full functionality within clients' systems.
Taxonomy search and alignment	Using the Elevate Standards Alignment taxonomies, both standards and content can be searched, and alignments can be created between them.
Alignment recommendations	Alignment recommendations are made using standards relationships, intermediaries, and machine learning; these recommendations can be used



Feature	Description
	to expand current alignment to other authorities or maintain alignment when new documents are adopted.
Content search	Tagged content can be smartly searched through the use of the AB Connect API.
Standards management	The system notifies users of new publications or documents within their license; changes to existing documents are tracked for ease of monitoring and maintenance of alignments. This information is available through the UI and through the API.
Interactive tagging and prediction application	The Alignment UIs enable efficient interactive tagging and alignment prediction review workflows. Flexible options include leveraging direct connection relationships (e.g. relating a Standard to an Asset), indirect references (e.g. relating entities based on mutual relationships with other entities), prediction (when the system suggests a relationship) and through other system derived means.
Multiple alignment solutions and applications/UIs	<p>Elevate Standards Alignment includes a system of both UIs and an API to offer solutions to help manage the ever changing world of standards.</p> <p>Monitoring and maintenance of the Academic Benchmarks repository of standards assures accurate and up-to-date standards data. Alignments can be easily maintained as changes to learning standards occur. One option is to use AB Connect's prediction algorithms, accessible both through the UIs and the API, which helps maintain alignments based on the content description rather than fixed relationships with specific standards.</p> <p>Another option is to use the Standards relationships available through the AB Connect API. AB Connect supplies maps from outdated Standards to</p>



Feature	Description
	their replacements as well as other relationships such as Derivatives and Crosswalks.
Workflow/project-management for alignments	Elevate Standards Alignment tools include a project-based system that allows for custom project setup, hierarchical levels of review, and user assignments and tracking.
Configurable reports	Configurable reports allow users to curate, review and format alignment related information created through the UIs, or the API. Multiple report types empower gap analysis, content review, and alignment reporting.



## Elevate Data Sync

Feature	Description
SIS Integration	Elevate Data Sync supports a growing number of industry-standard data models and protocols, such as OneRoster, LIS, SIF, APIs, and CSV, and utilizes the preferred integration method for each Student Information System (SIS) and application. This allows users to integrate with any SIS.
Application rostering	A Data Sync Integration is a plug-in you create and license to K12 and Higher Ed institutions to enable bi-directional synchronization between your application and their student information system (SIS).
Grade passback	The Grades Exchange API is used to exchange grade data between a grades producer, such as a learning management system (LMS), and a grades consumer, such as a student information system (SIS). Data Sync provides APIs to initiate a grades exchange and to implement the services of a Grades Producer and Grades Consumer.
Customizable validation and mapping	<p>A Data Validation Rule validates the value of an attribute. Objects with data validation errors are not allowed to pass downstream to the application. Use Data Validation rules to prevent data objects not meeting your API requirements from reaching your client app. For example, if your application requires that a person have an email address, you can create a data validation rule requiring that attribute to exist and to have a non-empty value.</p> <p>Mappings allow you to set the value of a new attribute, adjust the value of an existing attribute, or delete an attribute by invoking a scripting language such as Javascript. Mappings can be defined in an integration blueprint or at the individual customer level.</p>
Customizable roles and permissions	All actions that can be performed from the Dashboard are governed by user privileges. Privileges are organized into Roles that you assign to users:



Feature	Description
	Observer, Operator, Manager, Developer and Administrator. Higher level roles include all privileges from lower-level roles.
Supervisory controls	A partner can be granted supervisory access to their customers' accounts, allowing them to impersonate the account and manage it for the customer. These supervised organizations are listed in the partner's Supervisor list. Data Sync always obtains the organization's permission before granting supervisory access.
Mapping packages	A mapping package is a collection of mappings that can be applied to a customer account by installing the package rather than writing each individual mapping.
Publish and subscribe	Whenever a change is made to the Repository, all Integrations are notified of the change via the Publish & Subscribe Broker. The Broker is comprised of "actors"—Repositories, Connectors, and Integrations—that either publish or subscribe to "topics". Topics are organized into Data Models such as Rostering, Grades, and Attendance.
Transform data	During the transform step, raw data is transformed to the Data Sync data model. Mapping Rules of the Connector or Integration are used to transform from XML or JSON. All Connectors have factory defaults that produce the "Core Attributes" described in our Developer's Guide, but these rules can also be customized. Data can be transformed within the Repository and/or in-flight.
Scalability	Elevate Data Sync processes data in parallel while transforming it, which creates a highly scalable solution to securely share learning data and ensure students and teachers always have access to the applications they need while keeping their information safe.



Feature	Description
Command line interface tools	The command-line interface is an essential tool for developing and supporting Data Sync integrations; it can be used for querying data, scoping data, and troubleshooting.
API and explorer	The API Explorer allows developers to explore the different APIs, calls and functions that Data Sync supports.

## Elevate Data Quality

Feature	Description
Email Notifications	Assigned users receive email notifications about errors in data and data violations.
Validate data	As part of its certification process, Elevate Data Quality runs a battery of data certification rules each night against the student information system (SIS) and generates Scorecards that display which rules were violated by the data.
Data Prescriptions	User-created information that instructs users on how to rectify certain data errors.
Data Quality Scorecard	Quickly view the number and severity of data validation issues in composite with the Data Quality Scorecard.
Data Sync	Migrate data into the Data Quality module for data certification and validation.







**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:	<input 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 type="checkbox"/>
	Other assessment data-Please specify:	<input 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 checked="" type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input 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:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input checked="" type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input 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"/>
Parent / Guardian Name	First and/or Last	<input checked="" type="checkbox"/>
Schedule	Student scheduled courses	<input checked="" type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input checked="" type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify: Free or reduced lunch status	<input checked="" type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input checked="" type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input checked="" type="checkbox"/>
	Student course data	<input checked="" type="checkbox"/>
	Student course grades/ performance scores	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used By Your System
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data - Please specify:	<input type="checkbox"/>
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p>The Elevate products (Analytics and Sync) can process any SIS data described in the EdFi data schema as directed by the LEA.</p>	<input checked="" type="checkbox"/>
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 section.

**Originating LEA:** A local education agency 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 and/or Terms of Service and/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 Meta Data. 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 Education 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. 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.

**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."

**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

2/16/22  
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 2/7/2022, 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 five (5) 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:

privacy@instructure.com

PROVIDER: INSTRUCTURE, INC.

BY: Jeffrey Ebert Date: 02/10/2022

Printed Name: JEFF EBERT Title/Position: SR. MANAGER, DEAL DESK

**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

and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VI, SECTION 5. \*\***

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

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

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

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

**DESIGNATED REPRESENTATIVE OF LEA:**

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

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

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

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

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

**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)
<input checked="" type="checkbox"/>	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 checked="" 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.edspex.org> for further details about the noted frameworks.

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



**EXHIBIT "G"**

**Supplemental SDPC State Terms for California**

**Version 1.0**

This Amendment for SDPC State Terms for California ("**Amendment**") is entered into on February 7, 2022 (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 Instructure, Inc.

, located at 6330 S 3000 E, Ste. 700, Salt Lake City, UT 84121  
(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.

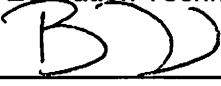
**Modification to Article IV, Section 7 of the DPA.** Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

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; 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.

**[SIGNATURES BELOW]**

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

LEA: Education Technology Joint Powers Authority

By:  Date: 2/16/22

Printed Name: Brianne Ford Title/Position: President

PROVIDER:

By: Daisy Bennett Date: 02/07/2022

Printed Name: Daisy Bennett Title/Position: Privacy Officer