

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 2.0 (July 3, 2018)

Capistrano Unified School District

AND

Discovery Education, Inc.

This California Student Data Privacy Agreement ("DPA") is entered into by and between the  
Capistrano Unified School District

(hereinafter referred to as "LEA") and Discovery Education, Inc.  
(hereinafter referred to as "Provider") on October 10, 2018. The Parties agree to  
the terms as stated herein.

### RECITALS

**WHEREAS**, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated June 6, 2017 ("Service Agreement"); and

**WHEREAS**, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

**WHEREAS**, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

**WHEREAS**, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to  
**ARTICLE I: PURPOSE AND SCOPE**

protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, 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. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

Digital curriculum services

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".
4. **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 term used in the Service Agreement.

## 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 Agreement 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 LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil 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 pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRa, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (4 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 data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected 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 state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRa, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (I), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and 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 LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

- a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

- b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

## ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
- f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance

monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

**2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty eight (48) hours. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
  - 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.
  - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c.** At LEA's discretion, the security breach notification may also include any of the following:
  - i.** Information about what the agency has done to protect individuals whose information has been breached.
  - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d.** Provider agrees to adhere to all requirements in applicable State and in federal law 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.



- e. 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 copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. 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 PRIVACY 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 this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

#### **ARTICLE VII: MISCELLANEOUS**

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .
2. **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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is



provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

**a. Designated Representatives**

The designated representative for the LEA for this Agreement is:

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

Contact Information:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

The designated representative for the Provider for this Agreement is:

Name: R. Brooks Garber \_\_\_\_\_  
Title: Counsel \_\_\_\_\_

Contact Information:  
One Discovery Place \_\_\_\_\_  
Silver Spring MD 20910 \_\_\_\_\_  
[counsel@discoveryeducation.com](mailto:counsel@discoveryeducation.com)

**b. Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: R. Brooks Garber \_\_\_\_\_  
Title: Counsel \_\_\_\_\_

Contact Information:  
One Discovery Place \_\_\_\_\_  
Silver Spring MD 20910 \_\_\_\_\_  
[counsel@discoveryeducation.com](mailto:counsel@discoveryeducation.com)

6. **Entire Agreement.** This DPA constitutes 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

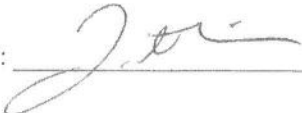
either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **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.
8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE IN WHICH THIS AGREEMENT IS EXECUTED, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **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.

*[Signature Page Follows]*

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

Discovery Education, Inc.

BY:  Date: October 10, 2018

Printed Name: Scott Kinney Title/Position: President, K-12

Capistrano Unified School District

BY:  Date: 11/1/18

Printed Name: Jeremy Davis Title/Position: CTO

*Note: Electronic signature not permitted.*

**EXHIBIT "A"**

DESCRIPTION OF SERVICES

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

Science Techbook is a breakthrough K-12 digital science textbook that changes the way students and teachers experience real-world science phenomena, boosting achievement and igniting interest in the exploration of cross-cutting science concepts.

Discovery Education Streaming Plus (DESP): Reimagine learning, ignite curiosity, and cultivate dynamic classrooms with DESP, the definitive collection of curated K-12 content collections and impactful instructional resources. This one-of-a-kind service has just what you're looking for. With just one click, access 180,000+ vetted resources, McRel International-aligned instructional strategies, a creation and collaboration space, and access to a worldwide professional learning community.

Social Studies Techbook is a comprehensive, standards-aligned, core curricular resource that uses an inquiry-based approach to enhance literacy and critical thinking skills. Courses in this digital social studies textbook include U.S. History, World History, Civics and Government, and World Geography and Cultures.

Math Techbook is a highly engaging, digital math textbook that connects students to math through real-world problems worth solving. Using a balanced approach to instruction, Math Techbook combines conceptual understanding, procedural fluency, and application to help all students develop a long-lasting mastery of mathematics.

STEM Connect encourages students to develop and apply solutions to real challenges facing the world. Relatable + Real The challenges posed to students progress from Grades K to 8. Younger students are faced with more personal, local issues. Whereas middle school students are pushed to solve more complex, global challenges. Students are also asked to personalize solutions to fit community and local needs.

■

**EXHIBIT "B"**

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system	Conduct	Conduct or behavioral data	
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	x	Demographics	Date of Birth	
	Other application technology meta data-Please specify:	Google Analytics, NewRelic		Place of Birth	
Application Use Statistics	Meta data on user interaction with application	x		Gender	
				Ethnicity or race	
Assessment	Standardized test scores			Language information (native, preferred or primary language spoken by student)	
	Observation data			Other demographic information-Please specify:	
	Other assessment data-Please specify:	x		Student school enrollment	
Attendance	Student school (daily) attendance data			Student grade level	x
	Student class attendance data			Homeroom	x
Communications	Online communications that are captured (emails, blog entries)			Guidance counselor	
			Specific curriculum programs		
			Year of graduation		
			Other enrollment information-Please specify:		
			Parent/Guardian Contact Information	Address	
				Email	x
				Phone	

Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
Schedule	Student scheduled courses	x
	Teacher names	x
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/ foster care)	
	Other indicator information- Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID	x

	number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	x
	Student app passwords	x
Student Name	First and/or Last	x
Student In App Performance	Program/appli- cation performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	x
Student work	Student generated content; writing, pictures etc.	
	Other student	

	work data - Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

	Other transportation data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

No Student Data Collected at this time \_\_\_\_\_.  
 \*Provider shall immediately notify LEA if this designation is no longer applicable.



## EXHIBIT "C"

### DEFINITIONS

**AB 1584, Buchanan:** The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

**Educational Records:** Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

**NIST:** Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

**Operator:** The term "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 primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

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

**Pupil Generated Content:** The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

**Service Agreement:** Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

**School Official:** For the purposes of this Agreement 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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

**SOPIPA:** Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

**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, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal 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.

**SDPC (The Student Data Privacy Consortium):** Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

**Student Personal Information:** "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

**Subprocessor:** For the purposes of this Agreement, 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 software, and who has access to PII.

**Targeted Advertising:** Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

**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 pupil records. However, for the purpose of this Agreement, 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

Capistrano Unified School District directs Discovery Education, Inc. to dispose of data obtained by Company pursuant to the terms of the Service Agreement between LEA and Company. The terms of the Disposition are set forth below:

<b><u>Extent of Disposition</u></b>	
Disposition shall be:	<input type="checkbox"/> Partial. The categories of data to be disposed of are as follows: <input checked="" type="checkbox"/> Complete. Disposition extends to all categories of data.
<b><u>Nature of Disposition</u></b>	
Disposition shall be by:	<input checked="" type="checkbox"/> Destruction or deletion of data. <input type="checkbox"/> Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
<b><u>Timing of Disposition</u></b>	
Data shall be disposed of by the following date:	<input checked="" type="checkbox"/> As soon as commercially practicable <input type="checkbox"/> By (Insert Date) _____

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

\_\_\_\_\_  
Date

\_\_\_\_\_  
Verification of Disposition of Data  
by Authorized Representative of Provider

\_\_\_\_\_  
Date

**EXHIBIT "F" DATA SECURITY REQUIREMENTS**

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

SEE ATTCHED - ATTACHMENT 1: DISCOVERY EDUCATION, INC.  
DATA SECURITY POLICY.



## ATTACHMENT 1

### DISCOVERY EDUCATION, INC. DATA SECURITY POLICY

This Policy describes, in general, (i) what steps Discovery Education, Inc. ("Discovery") takes to protect personally identifiable information ("PII") that is provided to Discovery; (ii) how PII may be used; (iii) with whom Discovery may share PII, and (iv) the steps Discovery takes to protect the PII.

No student PII is required for the use of any of the basic Discovery Education services, however, in the event Users elect to use any of the functionality within the Discovery Education services which provide personalized pages, individual accounts, other user-specific customization, or otherwise submit or upload information (all such data is generally limited to the following: school name, first name, last name, and grade level), all such PII provided to Discovery will be protected in accordance with this Policy.

No school employee PII is required for Professional Development Services other than first name and last name for the purposes of attendance logs.

#### I. DEFINITIONS

Capitalized terms referenced herein but not otherwise defined shall have the meanings as set forth below:

"Authorized Disclosee" means the following: (1) third parties to whom the Subscriber/Customer/Distributor has given Discovery written approval to disclose PII; (2) third parties to whom disclosure is required by law; and (3) if applicable, third party vendors working on Discovery's behalf or performing duties in connection with Discovery's services (e.g. hosting companies) to whom Subscriber/Customer/Distributor herein gives Discovery written approval to disclose PII received from Subscriber/Customer/Distributor and its Users and who are required to implement administrative, physical, and technical infrastructure and procedural safeguards in accordance with accepted industry standards.

"Authorized User" means a Discovery employee authorized by the Subscriber/Customer/Distributor to access PII in order to perform services under an Agreement.

"Destroy" or "Destruction" means the act of ensuring the PII cannot be reused or reconstituted in a format which could be used as originally intended and that the PII is virtually impossible to recover or is prohibitively expensive to reconstitute in its original format.

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, as they may be amended from time to time. The regulations are issued by the U.S. Department of Education, and are available at <http://www2.ed.gov/policy/gen/reg/ferpa/index.html>.

"Personally Identifiable Information" (or "PII") means any information defined as personally identifiable information under FERPA.

#### II. PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION

##### Basic Privacy Protections

1. **Compliance with Law and Policy.** All PII provided to Discovery is handled, processed, stored, transmitted and protected by Discovery in accordance with all applicable federal data privacy and security laws (including FERPA) and with this Policy.
2. **Training.** Employees (including temporary and contract employees) of Discovery are educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security.
3. **Personnel Guidelines.** All Discovery employees are required to be aware of and work to protect the confidentiality, privacy, and security of PII. Discovery, and its respective personnel do not access PII except to comply with a legal obligation under federal or state law, regulation, subpoena, or if there is legitimate need for the information to maintain data systems or to perform required services under the Agreement with Subscriber/Customer/Distributor. The following provides a general description of the internal policies to which Discovery and its respective personnel adhere:
  - a. Limit internal access to PII to Discovery personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel with a legitimate need for the PII to carry out



- the services provided under the Agreement.
- b. Disclose PII only to Authorized Disclosees.
  - c. Access PII only by Authorized Users.
  - d. When PII is no longer needed, delete access to PII.
  - e. Permit employees to store or download information onto a local or encrypted portable devices or storage only when necessary, and to create a written record for retention verifying that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).
  - f. Any downloaded materials consisting of PII remain in the United States.
  - g. Prohibit the unencrypted transmission of information, or any other source of PII, wirelessly or across a public network to any third party.
  - h. Upon expiration or termination of Agreement, Discovery shall Destroy all PII previously received from Subscriber/Customer/Distributor no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber/Customer/Distributor to Discovery to hold such PII. Each electronic file containing PII provided by Subscriber/Customer/Distributor to Discovery will be securely Destroyed. This provision shall apply to PII that is in the possession of Discovery, Discovery employees/personnel and/or Authorized Disclosees.

### **Information Security Risk Assessment**

Discovery periodically conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by Discovery; Discovery reports such risks as promptly as possible to Subscribers/Customers/Distributors; and Discovery implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented by Discovery based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

#### **1. Administrative Safeguards**

- a. **Sanctions:** Appropriate sanctions against Contractor personnel who fail to comply with Discovery's security policies and procedures.
- b. **System Monitoring:** Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
- c. **Security Oversight:** Assignment of one or more appropriate management level employees of Discovery to be responsible for developing, implementing, and monitoring of safeguards and security issues.
- d. **Appropriate Access:** Procedures to determine that the access of Discovery personnel to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Discovery personnel who have access to PII.
- e. **Employee Supervision:** Procedures for regularly monitoring and supervising Discovery personnel who have access to PII.
- f. **Access Termination:** Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

#### **2. Physical Safeguards**

- a. **Access to PII:** Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
- b. **Awareness Training:** On-going security awareness through training or other means that provide Discovery personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.
- c. **Incident Response Plan:** Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
- d. **Physical Access:** Procedures to limit physical access to PII and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.
- e. **Physical Identification Validation:** Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to the PII.
- f. **Operational Environment:** Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where PII is stored.





- g. **Media Movement:** Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.
3. **Technical Safeguards**
- a. **Data Transmissions:** Technical safeguards, including encryption, to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups.
  - b. **Data Integrity:** Procedures that protect PII maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.
  - c. **Logging off Inactive Users:** Inactive electronic sessions are designed to terminate automatically after a specified period of time.
  - d. **Data Backup:** Data is backed up daily and stored offsite for thirty days. In the event data has to be restored, data backups can be retrieved from offsite locations in one business day and the process of restoration would take an additional day.
  - e. **Disaster Recovery:** Disaster Recovery procedures are in place and are tested on a yearly basis. Discovery has two datacenters located in the United States that are utilized to recover operations.

### **Security Controls Implementation**

Discovery has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

### **Security Monitoring**

In combination with periodic security risk assessments, Discovery uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Discovery also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention.

### **Security Process Improvement**

Based on Discovery's security risk assessments and ongoing security monitoring, Discovery gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks, and new opportunities for managing security risks and incidents. Discovery uses this information to update and improve its risk assessment strategy and control processes.

### **Audit**

Discovery acknowledges Subscriber's/Customer's/Distributor's right to audit any PII collected by Discovery and/or the security processes listed herein upon reasonable prior written notice to Discovery's principal place of business, during normal business hours, and no more than once per year. Discovery shall maintain records and documentation directly and specifically related to the services performed under the Agreement for a period of three (3) years, unless otherwise stated in Section II (3)(h) of this Policy.

### **Breach Remediation**

Discovery keeps PII provided to Discovery secure and uses reasonable administrative, technical, and physical safeguards to do so. Discovery maintains and updates incident response plans that establish procedures in the event a breach occurs. Discovery also identifies individuals responsible for implementing incident response plans should a breach should occur.

If a Subscriber/Customer/Distributor or Discovery determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Discovery provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all breach of confidentiality laws.

Discovery reports as promptly as possible to Subscribers/Customers/Distributors (or their designees) and persons responsible for managing their respective organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of PII of which they become aware. Such incidents include any breach or hacking of Discovery's Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware



and software employed in Discovery's business, whether or not owned by Discovery or operated by its employees or agents in performing work for Discovery.

**Personnel Security Policy Overview**

Discovery mitigates risks by:

1. Performing appropriate background checks and screening of new personnel, in particular those who have access to PII.
2. Obtaining agreements from internal users covering confidentiality, nondisclosure and authorized use of PII.
3. Providing training to support awareness and policy compliance for new hires and annually for personnel.