CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

IRVINE UNIFIED SCHOOL DISTRICT

and

ILLUMINATE EDUCATION, INC.

February 14, 2018

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Irvine Unified School District (hereinafter referred to as "District") and Illuminate Education, Inc. (hereinafter referred to as "Illuminate") effective as of February 14, 2018 (the "Effective Date"). The parties agree to the terms as stated herein.

RECITALS

WHEREAS, Illuminate has agreed to provide District with access to and use of Illuminate's Data and Assessment Management System and certain other services (collectively, the "Services") pursuant to that certain DNA Software Services Agreement dated as of the Effective Date by and between Illuminate and District ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, Illuminate may receive and District may provide documents or data that are covered by several Federal and State statutes, among them, the Federal Educational and Privacy Rights Act ("FERPA") at 20 U.S.C. 1232g, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; and the Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data received by Illuminate from District are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 (sometimes referred to as "AB 1584") and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; 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.

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

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 transmitted to Illuminate from District pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. In performing the Services, Illuminate shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by District.

2. **Nature of Services Provided.** Illuminate has agreed to provide the Services as described in the Services Agreement.

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, District shall provide the categories of data as indicated in the Schedule of Data, attached hereto as Schedule "A".

4. **DPA Definitions**. The definition of certain terms used in this DPA is found in Schedule "B". In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of District**. All Student Data or any other Pupil Records transmitted to Illuminate pursuant to the Service Agreement is and will continue to be the property of and under the control of District. The parties agree that as between them, all rights, including all intellectual property rights in and to such Student Data or any other Pupil Records contemplated by the Service Agreement shall remain the exclusive property of District. Illuminate shall be considered a School Official, under the control and direction of District as it pertains to the use of Student Data notwithstanding the above. Pupils may retain possession and control of their own Pupil-Generated Content, and may transfer their own Pupil-Generated Content to a personal account, by submitting a written request directly to District. Illuminate may transfer Pupil-Generated Content to such a separate personal account, according to the procedures set forth below.

2. **Parent Access**. Illuminate shall assist District in establishing reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information 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 the Services. Illuminate shall respond in a reasonably timely manner to District's request for assistance in permitting the viewing or correcting of Personally Identifiable Information in Pupil Records held by Illuminate. In the event that a parent of a pupil or other individual contacts Illuminate to review any of the Pupil Records accessed pursuant to the Services, Illuminate shall refer the parent or individual to District, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Illuminate shall, at the request of District, assist District in the transfer of Pupil-Generated Content to a separate student account.

4. **Third Party Request**. Should a third party, including law enforcement and government entities, contact Illuminate with a request for Pupil Records held by Illuminate pursuant to the Services, Illuminate shall redirect the third party to request the Pupil Records directly from District. Illuminate shall notify District in advance of a compelled disclosure to a third party unless legally prohibited.

5. **No Unauthorized Use**. Illuminate shall not use Student Data or other information in a Pupil Record for any purpose other than those required or specifically permitted by the Service Agreement.

6. **Subprocessors**. Illuminate shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to be bound by the terms of this DPA.

ARTICLE III: DUTIES OF DISTRICT

1. **Provide Data In Compliance With FERPA**. District shall provide data for the purposes of the Service Agreement and comply with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. §1232 g, California AB 1584 and all other statutes and regulations pertaining to data privacy and security, including but not limited to FERPA, COPPA, PPRA, AB 1584, and SOPIPA.

2. **Reasonable Precautions**. District shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and Student Data to ensure that access of District users is limited to that portion of the Services and Student Data as is reasonably necessary in order to fulfill the purposes of the Services Agreement.

3. **Unauthorized Disclosure Notification**. District shall notify Illuminate promptly of any known or suspected unauthorized disclosure of Pupil Records. District will assist Illuminate in any efforts by Illuminate to investigate and respond to any unauthorized disclosure of Pupil Records.

4. **District Representative**. At the request of Illuminate, District shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF ILLUMINATE

1. **Privacy Compliance**. Illuminate shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including but not limited to FERPA, COPPA, PPRA, AB 1584, and SOPIPA.

2. **Authorized Use**. Pupil Records shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than those required or specifically permitted by the Service Agreement and/or otherwise authorized under the statutes referred to above.

3. **Employee Obligation**. Illuminate shall require all of its employees and agents who have access to Student Data to comply with all applicable provisions of FERPA with respect to the Pupil Records shared under the Service Agreement. Illuminate agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Pupil Records shared under the Service Agreement.

4. **No Disclosure**. Illuminate shall not disclose any Pupil Records obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. However, De-Identified Information may be used by Illuminate for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data**. Illuminate shall dispose of all Pupil Records obtained under the Service Agreement upon completion of the terms of the Service Agreement or upon the written request of District, and shall assist in the transfer of said data to District within 60

days of the date of termination of the Service Agreement and according to a schedule and procedure as the parties may reasonably agree. Nothing in the Service Agreement authorizes Illuminate to maintain Personally Identifiable Information obtained under the Service Agreement beyond the time period reasonably needed to complete such disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; or (2) erasing or otherwise modifying the Personally Identifiable Information in those records to make it unreadable or indecipherable. Upon request from District, Illuminate shall provide written notification to District when the Personally Identifiable Information has been disposed. The duty to dispose of Personally Identifiable Information shall not extend to De-Identified Information or data placed in a separate student account, pursuant to the other terms of the DPA. Nothing in the Service Agreement authorizes Illuminate to maintain Personally Identifiable Information beyond the time period reasonably needed to complete the disposition.

6. **Certification of Non-Retention**. Illuminate certifies that, in accordance with this DPA, Pupil Records will not be retained or available to Illuminate upon completion of the terms of the Service Agreement. This certification may be enforced through any lawful means, including but not limited to civil action.

7. **Advertising Prohibition**. Illuminate is prohibited from using Pupil Records to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by Illuminate; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Services to District.

ARTICLE V: DATA PROVISIONS

1. Data Security. Illuminate agrees to abide by and maintain commercially reasonable data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access**. Illuminate shall use commercially reasonable efforts to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data in compliance with Article 4.3 of NIST 800-63-3. Illuminate shall only provide access to Student Data to employees, agents and contractors who need access to fulfill Illuminate's obligations under the Service Agreement. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Data shall pass criminal background checks.

   b. **Security Protocols**. Both parties agree to maintain commercially reasonable security protocols in the transfer or transmission of any Student Data, including ensuring that such data may only be viewed or accessed by parties legally allowed to do so. Illuminate shall maintain all Student Data obtained from the District pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit such data obtained pursuant to the Service Agreement, except as necessary to perform the Services or fulfill the purpose of data requests by District.

c. **Employee Training.** Illuminate shall provide periodic security training to those of its employees who operate or have access to Illuminate's system used to provide the Services. Further, upon written request, Illuminate shall provide District with contact information of an employee who District may contact if there are any security concerns or questions.

d. **Security Technology.** The Services shall use Secure Socket Layer ("SSL"), or equivalent technology to protect Student Data from unauthorized access. The Services security measures shall include server authentication and data. Illuminate shall host Student Data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

e. **Security Coordinator.** Upon written request, Illuminate shall provide the name and contact information of Illuminate's employee responsible for security for the Student Data received pursuant to the Service Agreement.

2. **Unauthorized Disclosure.** In the event of unauthorized disclosure of Pupil Records held by Illuminate, Illuminate shall provide notification to District within a reasonable amount of time of the incident and, if required, District will notify affected parents, legal guardians or eligible students, as applicable, in writing of such unauthorized disclosure. Illuminate's notification to District shall include, to the extent reasonably available, the information required to be disclosed by District in any security breach notification required to be made by District pursuant to Section 1798.29 of the California Civil Code ("CC1798.29"), including but not limited to:

   i. A list of the types of PII that were or are reasonably believed to have been the subject of the unauthorized disclosure;

   ii. If the information is reasonably available at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the unauthorized disclosure, or (3) the date range within which the unauthorized disclosure occurred. The notification shall also include the date of the notice; and

   iii. A general description of the unauthorized disclosure, if that information is reasonably available at the time the notice is provided.

In addition, if District is required by CC1798.29 to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system and electronically submit a sample copy of that security breach notification, excluding any personally identifiable information, to the California Attorney General, Illuminate shall assist District in those efforts.

ARTICLE VI: MISCELLANEOUS

1. **Term.** The parties shall be bound by this DPA for the duration of the Service Agreement or so long as Illuminate maintains any Student Data shared under the Service Agreement.

2. **Priority of Agreements**. This DPA shall govern the treatment of Student Data and other Pupil Records in order to comply with applicable federal and state privacy protection laws, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this Section, all other provisions of the Service Agreement shall remain in effect, including but not limited to, any provisions relating to exclusion of damages or a cap on monetary liability.

3. Notice. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.

Irvine Unified School District	Illuminate Education, Inc.
Attn: Michelle Bennett	Attn: Contracts Administrator
5050 Barranca Parkway	6531 Irvine Center Drive, Suite 100
Irvine, CA 92604	Irvine, CA 92618

4. **Entire Agreement**. This DPA together with 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 CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN ORANGE COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA.

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

IRVINE UNIFIED SCHOOL DISTRICT

By: _____ Date: February 14, 2018

Printed Name: John Fogarty Title/Position: Asst. Supt Business Services

IUSD Board Approved 2/13/2018

ILLUMINATE EDUCATION, INC.

By: _____ Date: 1/8/18

Printed Name: Scott Hickson Title/Position: CFO

Note: Electronic signature not permitted.

SCHEDULE "A"

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.	✓
	Other application technology meta data-Please specify:	Optional
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	✓
	Observation data	✓
	Other assessment data-Please specify:	Optional
Attendance	Student school (daily) attendance data	Optional
	Student class attendance data	Optional
Communications	Online communications that are captured (emails, blog entries)	Optional
Conduct	Conduct or behavioral data	Optional
Demographics	Date of Birth	✓
	Place of Birth	✓
	Gender	✓
	Ethnicity or race	✓
	Language information (native, preferred or primary language spoken by student)	✓
	Other demographic information-Please specify:	Optional
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	✓
	Guidance counselor	Optional
	Specific curriculum programs	Optional
	Year of graduation	Optional
	Other enrollment information-Please specify:	Optional
Parent/Guardian Contact Information	Address	Optional
	Email	Optional
	Phone	Optional
Parent/Guardian ID	Parent ID number (created to link parents to students)	Optional
Parent/Guardian Name	First and/or Last	Optional

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	✓
	Teacher names	✓
Special Indicator	English language learner information	✓
	Low income status	Optional
	Medical alerts	Optional
	Student disability information	Optional
	Specialized education services (IEP or 504)	Optional
	Living situations (homeless/foster care)	Optional
	Other indicator information-Please specify:	Optional
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	Optional
	Email	Optional
	Phone	Optional
Student Identifiers	Local (School district) ID number	✓
	State ID number	✓
	Vendor/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	✓
Student Survey Responses	Student responses to surveys or questionnaires	✓
Student work	Student generated content; writing, pictures etc.	✓
	Other student work data - Please specify:	Optional

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	Optional
	Student course data	Optional
	Student course grades/performance scores	Optional
	Other transcript data -Please specify:	Optional
Transportation	Student bus assignment	Optional
	Student pick up and/or drop off location	Optional
	Student bus card ID number	Optional

Category of Data	Elements	Check if used by your system
	Other transportation data - Please specify:	Optional
Other	Please list each additional data element used, stored or collected by your application	We collect thousands of data points, but nothing beyond the pii elements above

SCHEDULE "B"

DEFINITIONS

De-Identified Information (DII): De-Identified Information means data from which Illuminate has removed or obscured 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.

NIST 800-63-3: NIST 800-63-3 means draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 177, SOPIPA, 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 "Illuminate." This term shall encompass the term "Third Party," as it is found in AB 1584.

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 Illuminate's software, website, service, or app, including mobile apps, whether gathered by Illuminate or provided by District or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

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: The term "Pupil Records" means both of the following: (1) Any information that directly relates to a pupil that is maintained by District 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 District employee.

School Official: For the purposes of this DPA and pursuant to 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 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Illuminate or provided by District 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 identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this DPA. Student Data as specified in Exhibit A is confirmed to be collected or processed by Illuminate pursuant to the Services. Student Data does not include information that has been anonymized or de-identified.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than District or Illuminate, who Illuminate uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII. This term shall also include service providers covered by SOPIPA.

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 Illuminate'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" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) 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 DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Illuminate."