

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Tustin Unified School District

and

BrainPOP LLC

08/24/2017

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

Described in 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 or any other Pupil Records 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 Parties agree that as between them all rights, including all intellectual property rights in and to Student Data or any other Pupil Records 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 personally identifiable information on 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 reasonably timely manner to the LEA's request for personally identifiable information 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 Pupil Records of 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.** Provider shall, at the request of the LEA, transfer Student generated content to a separate student account.
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 unless legally prohibited.

4. **No Disclosure.** Provider shall not disclose any data 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. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data.** Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the 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. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition.** Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families/guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures 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 in Exhibit "D" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by 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. 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 Records shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was

- 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. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.
- e. At the request and with the assistance of the District, 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.

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 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. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
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.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall

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 SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[Signature Page Follows]

EXHIBIT "A"

DESCRIPTION OF SERVICES

Subscription services to online educational content (including one or more of the following: BrainPOP, BrainPOP Jr, BrainPOP Espanol, BrainPOP Francais, BrainPOP ESL)

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	<input checked="" type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data -Please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if used by your system
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	Please list each additional data element used, stored or collected by your application	<input checked="" type="checkbox"/>

automatically by these third parties. If you want to opt out of third party cookies, you may do so through your browser, as mentioned above in **Information collected automatically**.

Information collected when using My BrainPOP®: School, District and Homeschool subscriptions include the option to use the individual accounts system, called My BrainPOP, which allows students and their teachers to keep track of learning. Student and teacher accounts are organized by classrooms created by the teachers of the subscribing school. For these accounts, we ask the teachers to enter the first and last name of students and teachers, their username, the class they are associated with and a security question for resetting their password. We also require the teachers' email for password recovery and for contacting them on support and service-related announcements. The only Personally Identifiable Information collected about students is their name, class, graduation year, and the students' work under the account (student records). If a student uses the Make-a-Movie™ feature, his or her recorded voice may also be collected as part of the movie file that will be saved. We do NOT collect students' emails or addresses. We store the data created in each student account ("Student Records"), such as the history of BrainPOP movies they've watched, the quizzes and activities they've completed, snapshots they've taken on certain GameUp® games, movies they've created using Make-a-Movie, and feedback provided by the teacher to the student through My BrainPOP. We do so for the purpose of enhancing teachers' and students' use of the website. Please see the [Using My BrainPOP®](#) section below for additional privacy and security information for users of My BrainPOP.

Contact information for newsletter and surveys: On BrainPOP Educators®, a section of these websites that is directed to adults, you may choose to register to receive newsletters, promotional offerings or surveys, which requires your contact information. Such messages may include pixel tags and link tracking. The contact information you submit will not be shared, sold or used for any other purpose and you may opt out at any time. An opt-out link will be included in the bottom of such messages. Registration to newsletters, promotional offering and surveys is not intended for minors under the age of 13. Please see [BrainPOP Educators®](#) below for further information.

Emails received from users: We may retain certain information from users when they send us messages through our system or by email. We only use such information for providing the services or support requested.

Feedback: Certain features we offer include an option to provide us with feedback on your experience. The feedback feature does not identify the user submitting it. The feedback option is voluntary and the information a user submits to us will only be used for improving these features. If we receive personally identifiable information through a feedback form we take steps to immediately delete that information.

Information collected when using a BrainPOP® mobile app: Your website subscription may also provide access to the Full Access level of our mobile apps. If you choose to download any such app and log into it with your website subscription username and password, we collect limited usage information in connection with user logins in order to monitor subscription compliance. This information is maintained in accordance to this policy. We do not collect Personally Identifiable Information from users of the various BrainPOP applications. If you subscribe to a BrainPOP app with an in-app purchase subscription, we do not collect any user information.

Push Notifications on mobile apps: We send you push notifications on BrainPOP mobile apps from time to time in order to update you about any events or promotions that we may be running. If you no longer wish to receive these types of communications, you may turn them off at the device level. To ensure you receive proper notifications, we will need to collect certain information about your device such as operating system and user identification information. We also collect the user timezone as it's set on the

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.

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

Operator: For the purposes of SB 1177, 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 "Provider." 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 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, 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

analytics, storage, or other service to operate and/or improve its software, and who has access to PII. This term shall also include in it meaning the term "Service Provider," as it is found in 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 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.

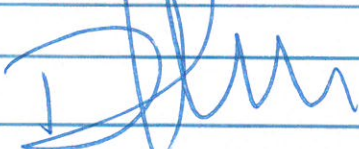
Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and BrainPOP LLC and which is dated August 24, 2017 to any other LEA ("Subscribing LEA") to anyone who accepts this 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 other LEA may also agree to change the data provided by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Tustin Unified School District



Printed Name:

David D. Smith

Date:

9-12-17

Title/Position:

CTO

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. *and attached Additional Terms/Deviations.*

BrainPOP LLC

Avraham Kadar.

Printed Name:

Dr. Avraham Kadar

Date:

9/12/17

Title/Position:

CEO and founder

**ADDITIONAL TERMS AND DEVIATIONS TO THE CALIFORNIA STUDENT DATA PRIVACY AGREEMENT
WITH TUSTIN UNIFIED SCHOOL DISTRICT**

Article II

Section 1, Student Data Property of LEA - Add: "Student Data and Pupil Records shall not include anonymous or de-identified information."

Section 5, No unauthorized use- Add: "or Terms of Use." (See Terms of Use definition below)

Article IV

Section 1, Privacy Compliance – Add "The Provider shall comply with all *applicable* California and Federal laws..."

Section 4, No Disclosure – Add: "De-identified and anonymous information may also be used for the purposes as outlined in the Terms of Use."

Section 5, Disposition of Data- Delete and add the following: "Each school or District has access to a user-friendly administrator dashboard that allows direct control over the Student Records at all times. The administrator can create, update, review, modify and delete individual accounts, and monitor logins in the individual accounts. "Administrators" are only those individuals explicitly designated by the school or the District. District and schools are able to delete information at any time and in real time using the Administrator Dashboard. Once information is deleted, LEA does not retain any copies. Teachers may also choose to archive the classroom they created. My BrainPOP classrooms that have been archived are retained for a period of two years. After such period, all information is automatically disposed and deleted; first it is deleted from the server and two weeks thereafter it is deleted from any backup server and cannot be restored."

Article V

Section 1(b), Destruction of Data – Delete and add the following: "District has full control over the personally identifiable data through the Administrator Dashboard and can delete the information at any time."

Article VII

Section 7, Entire Agreement – Add after "This DPA...": "and the Terms of Use"

Section 9, Governing Law; Venue and Jurisdiction – Add: "Notwithstanding the foregoing, any claim in connection with this Agreement must first, and before taking any other legal action, be submitted to Vendor in the form of a complaint (to: info@brainpop.com), to enable the parties to resolve the claim in