

**CALIFORNIA STUDENT DATA PRIVACY AGREEMENT**  
**Version 1.0**

Capistrano Unified School District

**and**

BrainPOP LLC

11/02/2017

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Capistrano Unified School District (hereinafter referred to as "LEA") and BrainPOP LLC (hereinafter referred to as "Provider") on November 3, 2017. 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 November 3, 2017 ("Service Agreement"); and

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

**WHEREAS**, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 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; and

**WHEREAS**, the Provider may, by signing the "General Offer of Privacy Terms", agrees 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:

**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 Provider from the LEA 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 these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
  
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

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":

See 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.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree protect Student Data in manner consistent with the terms of this DPA

#### ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA.** LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **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.
4. **District Representative.** At request of Provider, LEA 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 PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, AB 1584, and SOPIPA.
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 (1), above.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider 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

obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices 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 computer 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, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
  - f. **Security Coordinator.** 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.
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. 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. 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

destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, 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 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, 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.
6. **Application of Agreement to Other Agencies.** Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.
7. **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.
8. **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.
9. **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 SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

*[Signature Page Follows]*

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

Capistrano Unified School District

*Phillipa Townsend*

Date: 11/02/2017

Printed Name: PHILIPPA TOWNSEND

Title/Position: ASST SUPT., FISCAL

BrainPOP LLC

*Avraham Kadar.*

Date: 11/02/2017

Printed Name: Dr. Avraham Kadar

Title/Position: CEO & Founder

*Note: Electronic signature not permitted.*

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

BrainPOP  
BrainPOP Jr.  
BrainPOP Espanol  
BrainPOP Francais  
BrainPOP Educators

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

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

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

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"/>

## EXHIBIT B – “OTHER”

We collect the following types of information:

**Information collected when subscribing:** In the registration process of any of our subscription types, we ask our subscriber to provide us with name, email address, affiliation with a school or district (if applicable), phone number and billing information. We use this contact information to send users service-related announcements on rare occasions when it is necessary or advisable to do so. For instance, if we perform routine maintenance, we might send an informational email. We may also use this contact information to request feedback on the use of our products and services, to be used to improve the products and services. We will always provide an option to opt out of such communications.

**Username and password:** Subscribers create a username and password in the registration process, or, if they prefer, we may assign these for them. We use usernames and passwords of subscribers' accounts to authenticate logins, allow access to the paid content and monitor subscription compliance. The username is also used to authenticate users when requesting technical support. The passwords are all encrypted when stored. For more information on our security practices, see "How We Store and Process Your Information" below.

**Information collected automatically:** We automatically receive and record information on our server logs from a user's browser, including the user's IP address. We use IP addresses to maintain a user's session and we do not store them after the user's session is over. We also use the IP address to check if a user is located in some countries outside of the United States where a country-wide log-in option is activated, and we do not store this information after the initial page load. We do not otherwise combine this information with other PII.

We also use a standard feature found in browser software, called a "cookie", in order to establish and authenticate user sessions, enable access to paid content and monitor potential misuse of the accounts. We do not use cookies to collect Personally Identifiable Information nor do we combine such general information with other PII to identify a user. Disabling our cookies will prevent access to paid content and limit some of the features and functionalities of the website or app. To learn more about browser cookies, including how to manage or delete them, look in the Tools, Help or similar section of your Web browser, or visit [allaboutcookies.org](http://allaboutcookies.org).

We do not collect a user's web search history across third party websites or search engines. However, if a user navigates to our website via a web search, their web browser may automatically provide us with the web search term they used in order to find our website. Our website does not honor "do not track" signals transmitted by users' web browsers, so we encourage you to visit these links if you would like to opt out of certain tracking: <http://www.networkadvertising.org/choices> or <http://www.aboutads.info/choices/>. If you do want to opt out using these tools, you need to opt out separately for each of your devices and for each web browser you use (such as Internet Explorer®, Firefox® or Safari®) on each device.

**Third Parties:** We may use a variety of third-party service providers, such as analytics companies, to understand usage of our services. We may allow those providers to place and read their own cookies, electronic images known as web beacons or single-pixel gifs and similar technologies, to help us measure how users interact with our services. This technical information is collected directly and

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

device to limit the time we send push notifications within a reasonable time of day. We do not combine this information with other PII.

**Mobile Analytics on mobile apps:** We use mobile analytics software to allow us to better understand the functionality of our Mobile apps Software on your phone. This software may record information such as how often you use the apps, the events that occur within the apps, aggregated usage, performance data, and where the apps were downloaded from. We do not link the information we store within the analytics software to any PII you submit within the mobile apps.

**We Do NOT Collect Or Use Information As Follows:**

- Certain activity pages and quizzes allow a user to enter his or her name prior to printing or sending it to an email address entered by the user (such as that of a teacher). We do not collect or store this information. If a user is using a quiz on an app, he or she can enter their name, but we do not collect this information. It is only stored on the user's device.
- Other than in the places and for the purposes explicitly disclosed in this Policy, we do not knowingly collect Personally Identifiable Information directly from users under the age of 13. If we learn that we have inadvertently collected any Personally Identifiable Information from a user under 13, we will take steps to promptly delete it. Please contact us at [privacy@brainpop.com](mailto:privacy@brainpop.com) if you believe we have inadvertently collected Personally Identifiable Information from a user under 13.
- We do not collect, use or share Personally Identifiable Information other than as described in our privacy policy, or with the consent of a parent or legal guardian as authorized by law, or otherwise as directed by an applicable district or school or required by contract or by law.
- In no event shall we use, share or sell any Personally Identifiable Information for advertising or marketing purposes.



## 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

## Information in the Student's Email

**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 Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

**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 local educational LEA employee.

**SB 1177, SOPIPA:** Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

**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 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 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.

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

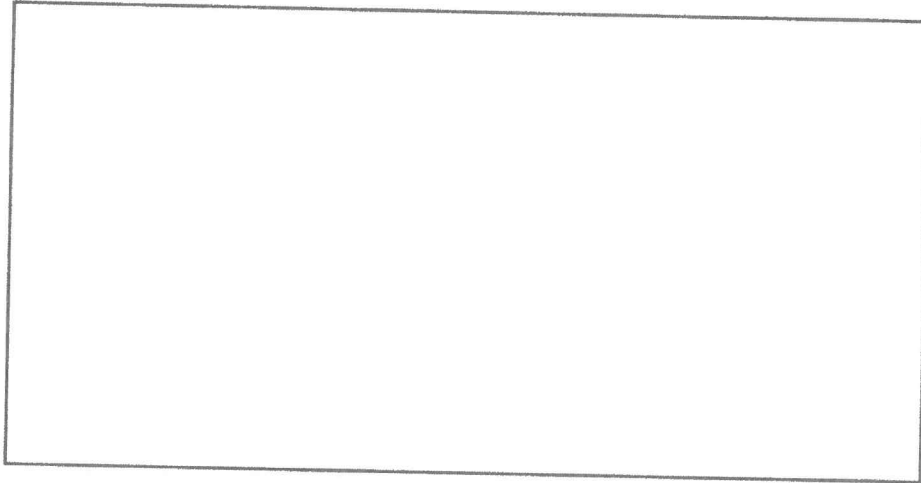
**Subprocessor:** For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection,

analytics, storage, or other service to operate and/or improve its software, and who has access to PII. 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 "D"**  
**DATA SECURITY REQUIREMENTS**



**EXHIBIT "E"**

**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Capistrano Unified School District and which is dated November 2, 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.

BrainPOP LLC

Avraham Kadar.

Date: 11/2/2017

Printed Name: Dr. Avraham Kadar

Title/Position: CEO & Founder

**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.

Date:

Printed Name:

Title/Position:

00618-00001/3519835.1

**ADDITIONAL TERMS AND DEVIATIONS TO THE CALIFORNIA STUDENT DATA PRIVACY AGREEMENT  
WITH CAPISTRANO 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, Provider 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. All student data will be deleted after a period of two years after expiration or termination of the applicable subscription. "

**Article V**

Section 1(a) Passwords and Employee Access – Delete "at a level by Article 4.3 of NIST 800-63-3."

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 1, Termination – Delete "Service Agreement" and replace with "the applicable subscription"

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](mailto:info@brainpop.com)), to enable the parties to resolve the claim in a friendly and effective manner. Notwithstanding the foregoing, LEA may seek injunctive or other equitable relief to protect its intellectual property rights in any court of competent jurisdiction.”

**Additional Terms to DPA:**

The use of the BrainPOP Products shall be governed by the Terms of Use, the User Agreement and the Privacy Policy, as posted on the website [www.brainpop.com](http://www.brainpop.com) and as updated from time to time (the “Terms of Use”). This Agreement will form an integral part of the Terms of Use for the District and the schools subscribing. Unless expressly changed herein, all other terms and conditions of the Terms of Use, as updated from time to time, shall not be affected, and shall remain in full force and effect. In any contradiction or discrepancy between the terms of this Agreement to those of the Terms of Use, as updated from time to time, the terms of this Agreement shall prevail for the term of the applicable subscription.