WASHINGTON STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Monroe School District

And

BrainPOP LLC

5/9/2019

This Washington Student Data Privacy Agreement ("DPA") is entered into by and between the Monroe School District (hereinafter referred to as "LEA") and BrainPOP LLC (hereinafter referred to as "Provider") on 5/9/2019. 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 the Terms of Use and Privacy Policy that govern the use of Provider's products, as posted on www.brainpop.com as updated from time to time ("Service Agreement"); and

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

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several Washington State privacy laws, including Student User Privacy in Education Rights ("SUPER") 28A.604.010 *et seq.*, as well as RCW 19.255.010 *et seq.* and RCW 42.56.590.

WHEREAS, for the purposes of this DPA, Provider is a School Official with legitimate educational interests in accessing educational records and performing Services pursuant to the Service Agreement; and

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

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Washington 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 statutes, including the FERPA, PPRA, COPPA, SUPER and other applicable Washington State laws, all as may be amended from time to time. In performing these Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

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

Enter a brief description of products and services.

BrainPOP, BrainPOP Jr, BrainPOP ELL, BrainPOP Espanol, BrainPOP Francais

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

4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C" attached hereto. 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 LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer student-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the student's records, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of Services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information. Student Data shall not include anonymous or de-identified information.

3. **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 unless legally prohibited. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

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

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data to Provider for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SUPER and all other applicable Washington privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 4 CFR § 99.31 (a) (1), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to its computer systems, Services and hosted data.

4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SUPER and all other applicable Washington privacy statutes.

2. **Authorized Use.** The data shared pursuant to the Service Agreement, including Persistent Unique Identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation.** Provider shall require all officers, employees and agents (including, but not limited to, Subprocessors) who have access to Student Data to comply with all applicable provisions of the Service Agreement with respect to the data shared under the applicable subscription.

4. **No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, Services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA, which has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement. De-identified information and anonymous information may also be used and shared with third party web analytical tools for tracking analytical information and also may be used and shared for educational research purposes and to evaluate, inform or show the efficacy of Provider's services.

5. **Disposal of Data.** Each school or District has access to a user-friendly administrator dashboard that allows direct control over the Student Data at all times. The administrator can create, update, review, modify and delete individual accounts, and monitor logins in the individual accounts. 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. 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.

a. Partial Disposal During Term of Service Agreement. Throughout the term of the Service Agreement, LEA is in full control over the data at all times and can delete the Student Data at any time. Once deleted by LEA, it will be purged from Provider's servers within 2 weeks.

b. Complete Disposal Upon Termination of Service Agreement. Prior to the termination or expiration of the subscription, LEA may delete all Student Data obtained under the Service Agreement.

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

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and commercially reasonable practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" attached hereto. These measures shall include, but are not limited to:

a. Passwords and Employee Access. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at industry standards. Provider shall only provide access to Student Data to employees, contractors and/or Subprocessors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with applicable state and federal ordinances.

b. Destruction of Data. Provider shall destroy or delete all Student Data obtained under the subscription when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond two years following the termination or expiration of the subscription. . However, LEA can delete the Student Data at any time. Once deleted by LEA, it will be purged from Provider's servers within two weeks.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or who are authorized to access the Provider's computer systems and/or the Student Data. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. Mobile Use of Student Data. Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of Student Data by Provider's employees, contractors and/or Subprocessors shall be protected by industry standard encryption to prevent unauthorized access by third parties. Provider shall also implement a Bring Your Own Device ("BYOD") policy for its own employees, which requires them to use physical and technical safeguards against third party access to the device, and a copy of that BYOD policy shall be provided to LEA as part of Exhibit F to this DPA. Provider shall ensure that all contractors and/or Subprocessors that have direct access to Student Data implement BYOD policies, which provide for substantially the same level of security for mobile devices as are provided by Provider's BYOD policy.

f. **Security Technology**. When the Student Data is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

g. Security Coordinator. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

h. Subprocessors Bound. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the Service Agreement. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance.

I. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. In the event that the term of the Service Agreement is anticipated to be longer than two (2) years, Provider shall provide written confirmation to the LEA that a third party has conducted a risk assessment analysis of Provider's computer systems at some point during the term of the subscription, upon LEA's written request.

j. Compliance Audit. LEA shall have the right but shall be under no obligation to conduct audit(s), from time to time, of Provider's records concerning its compliance obligations as set forth in this Article V. Provider shall make such records and other documents available to LEA upon request. The right to audit shall be subject to the following: LEA's right to audit shall only apply to Operator's books, records and documents that are directly related to the DPA or to the LEA, and the number of audits shall be limited to no more than once per year.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA promptly following discovery 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 , the following information if applicable:

i. The name and contact information of the reporting Provider subject to this section

ii. A list of the types of Student Data 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 and the law enforcement agency determined that notification would impede a criminal investigation.

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 Provider has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects commercially reasonable practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI – INDEMNITY

1. Indemnity. Provider shall defend, indemnify and hold harmless the LEA, its officers, directors, employees, agents and assigns (the "Indemnitees") from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance carrier, arising out of or resulting from any third-party claim against the Indemnitees arising out of or resulting from Provider's failure to comply with any of its obligations under this DPA. Provider's duty to defend and indemnify the LEA includes any and all claims and causes of action whether based in tort, contract, statute, or equity. Provider agrees that it shall be obligated to accept any tender of defense by the LEA pursuant to this DPA and provide a full defense to the LEA so long as any potential exists for Provider to have an obligation to indemnify the LEA for any part of any potential judgment against the LEA.

Provider's defense and indemnity obligations herein are intended to provide for the broadest indemnity rights available under Washington law and shall survive the termination of this DPA. To the extent Provider's defense and indemnity obligations as set forth in this DPA conflict with the terms of the Service Agreement, the defense and indemnity provisions set forth herein shall control.

The indemnities set forth herein shall be limited to the amounts covered by insurance and subject to the following: LEA shall provide Provider with (a) prompt written notice of such claim; (b) the right to solely control and direct the investigation, preparation, defense and settlement thereof, and (c) reasonable assistance and information.

ARTICLE VII- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VIII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the subscription or so long as the Provider maintains any Student Data.

2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the subscription has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach by Provider, its employees, or agents of the terms of this DPA.

3. **Effect of Termination Survival.** If the subscription is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. No indemnification provisions granted by the LEA in the Service Agreement shall be effective as to a breach of the terms of this DPA by the Provider. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this DPA is:
Name: Rachelle Butz Title: Executive Director of Digital Learning and Infrastructure

Contact Information: butzr@monroe.wednet.edu
200 East Fremont St, Monroe, WA 98272
360-804-2570

The designated representative for the Provider for this DPA is:

Name: Legal Department Title: ____________________

Contact Information:

legal@brainpop.com
____
____

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

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

Name: Legal Department Title: _______________

Contact Information:

legal@brainpop.com
____
____

6. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WASHINGTON, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY. NOTWITHSTANDING THE FOREGOING, ANY CLAIM IN CONNECTION WITH THIS AGREEMENT MUST FIRST, AND BEFORE TAKING ANY OTHER LEGAL ACTION, BE SUBMITTED TO OPERATOR IN THE FORM OF A COMPLAINT (TO: 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.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **Successors Bound.** This DPA is and shall be binding upon Provider's respective successors in interest in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this Washington Student Data Privacy Agreement as of the last day noted below.
Name of Provider: BrainPOP LLC

By: Avraham Kadar. Date: 5/9/2019 [redacted]

Printed Name: Dr. Avraham Kadar Title/Position: CEO and Founder

Address for Notice Purposes:

71 W 23rd St, 17th floor
New York, NY 10010 or legal@brainpop.com

Name of Local Education Agency: Monroe School District

By: Date: 09/01/2019

Printed Name: Rachelle Butz Title/Position: Exc. Dir. of Digital Learning

Address for Notice Purposes:

butzr@monroe.wednet.edu, 200 East Fremont St., Monroe, WA 98272

Note: Electronic signature not permitted.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Subscription services to online educational content: BrainPOP, BrainPOP Jr., BrainPOP ELL, BrainPOP Espanol, and BrainPOP Francais

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.	x
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
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:	

Category of Data	Elements	Check if used by your system
Enrollment	Student school enrollment	
	Student grade level	x
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	x
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	x
	State ID number	
	Vendor/App assigned student ID number	x
	Student app username	x
	Student app passwords	x
Student Name	First and/or Last	x
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.	x
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	

Category of Data	Elements	Check if used by your system
Transportation	**Student bus assignment**	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please specify:	
Other	**Please list each additional data element used, stored or collected by your application**	x

No Student Data Collected at this time ________

*Provider shall immediately notify LEA if this designation is no longer applicable.

EXHIBIT B – "OTHER"

We collect the following types of information:

Information collected during subscription process: During the registration process for any of our subscription types, we ask the subscriber to provide us with a name, email address, school or district affiliation (when applicable), phone number, and billing information. We use the contact information to send users service-related announcements. For instance, we may send emails about routine maintenance or new feature launches. We may also use this contact information to request feedback on our products and services, to inform future customer service and product improvements. All such communications include an opt-out feature.

Username and password: Subscribers may create a username and password during the registration process, or, if they prefer, we can assign these credentials. We use subscribers' usernames and passwords to authenticate log-ins; allow access to the paid content; and monitor subscription compliance. The username is also used to authenticate users when they request technical support. 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 has ended. We also use the IP address to see whether a user is located outside of the United States, where a country-wide log-in option is activated. We do not store this information beyond the initial page load, and we do not otherwise combine this information with other PII.

We also use cookies, a standard feature found in browser software, in order to establish and authenticate user sessions, enable access to paid content, and monitor potential account misuse. We do not use cookies to collect personally identifiable information and we do not 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 functionalities within our website(s) or app(s). To learn more about browser cookies, including how to manage or delete them, look in the Tools or Help section of your Web browser, or visit allaboutcookies.org.

We do not collect users' 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 us. Our website does not honor "do not track" signals transmitted by users' web browsers, so we encourage you to visit the following link if you would like to opt out of certain tracking: http://www.networkadvertising.org/choices or http://www.aboutads.info/choices/. Note that if you wish to opt out, you will need to do so separately for each of your devices and for each web browser you use (such as Internet Explorer®, Firefox®, Safari®).

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 wish 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 of using My BrainPOP, our individual accounts system, which allows students and their teachers to keep track of learning. Student and teacher accounts are organized into classrooms created by the teachers of the subscribing school. For these accounts, we ask teachers to enter their first and last name and their students'; their username; the class with which they are associated; and a security question for use if they need to reset their password. We also require the teachers' email for password recovery and for sending notifications or messaging about new features, product use recommendations, efficiency testing, backup schedules, survey and research participation invitations, and more (messaging may not be available in all jurisdictions). An opt-out link will be included at the bottom of messages that are not solely operational. The only Personally Identifiable Information collected about students is their name, class, graduation year, and work associated with 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 teacher and student use of the website. Please see the Using My BrainPOP® section below for additional privacy and security information pertaining to My BrainPOP.

We Do NOT Collect or Use Information As Follows:

Certain activity pages and quizzes allow users to enter their names prior to printing or emailing (to a teacher, for example). We do not collect or store this information. A user may enter his or her name when taking a quiz on an app, but we do not collect it. That information 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. If you believe we have inadvertently collected personally identifiable information from a user under 13, please contact us at privacy@brainpop.com.

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 as required by contract or by law.

In no event shall we use, share or sell any student Personally Identifiable Information for advertising or marketing purposes.

How We Share Your Information

We may provide Personally Identifiable Information to our partners, business affiliates, and third party service providers who work for BrainPOP and operate some of its functionalities - these may include hosting, streaming, and credit card processing services. A current list of these third parties is available upon request through privacy@brainpop.com. These third parties are well-known, established and/or vetted providers, who are bound contractually to practice adequate security measures and to use your information solely as it pertains to the provision of their services. They do not have the independent right to share your personally identifiable information. We share anonymous or de-identified information about our users when they are using third party web analytical tools, for tracking analytical information. We may use or share anonymous or aggregate and de-identified information for educational research purposes, to evaluate, inform, or show the efficacy of our services.

We will NOT share any personally identifiable information for marketing or advertising purposes.

EXHIBIT "C"

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the States of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs as identified by Washington Compact Provision 28A.705.010. The categories of Educational Records under Washington law are also found in Exhibit B. For purposes of this DPA, Educational Records are referred to as Student Data.

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.

Indirect Identifiers: Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator (*e.g.*, state, county) and other descriptors.

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

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Data Privacy Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term

"Third Party," as it is found in applicable state statutes.

Persistent Unique Identifiers. A long-lasting identification for digital objects, which allows for those digital objects to be located even if they are moved or removed.

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

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

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

Service Agreement: Refers to the Terms of Use and Privacy Policy that govern the use of Provider's products, as posted on www.brainpop.com and as updated from time to time.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

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 identities, 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 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.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student 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 student content.

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

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to Student Data.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the

Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSAL OF DATA

Monroe School District (hereinafter referred to as "LEA") directs Brainpop (hereinafter referred to as "Provider") to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. Unless modified by separate agreement pursuant to a pre-termination data disposal meeting as described in Article IV Section 5(c), the terms of the Disposal are set forth below:

Extent of Disposal	Disposal shall be:		**Partial.** The categories of data to be disposed of are set forth in an attachment to this directive.
			Complete. Disposal extends all categories of data.
Nature of Disposal	Disposal shall be by:		**Destruction or deletion of data.**
			Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
Timing of Disposal	Data shall be disposed of by the following date:		**As soon as commercially practicable**
			By (Insert Date) 60 days after termination of services
		Completed transfer and disposal of data shall occur no more than 60 days.	

Authorized Representative of LEA　　　　Date

Verification of Disposal of Data by Authorized Representative of Provider　　　　Date

EXHIBIT “E”

GENERAL OFFER OF PRIVACY TERMS Monroe School District

1. Offer of Terms Provider offers the same privacy protections found in this DPA between it and Monroe School District and which is date 09/01/2019 to any other LEA (“Subscribing LEA”) 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 subject listed in the Originating Service Agreement; or three (3) years after the date of Provider’s signature to this Form. Provider shall notify ACPE in the event of any withdrawal so that this information may be transmitted to the Alliance’s users.

BrainPOP LLC

By: Avraham Kadar. Date: 5/9/2019

Printed Name: Dr. Avraham Kadar Title/Position: CEO and 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.

Monroe School District

By: ____________________ Date: __________

Printed Name: ____________________ Title/Position: __________

<u>TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW</u>

Name: ____________________

Title: ____________________

Email Address: ____________________

EXHIBIT “F”

DATA SECURITY REQUIREMENTS

No additional data security requirements needed beyond what is stated in above information