TEXAS DATA PRIVACY AGREEMENT/ADDEDNUM TO SERVICE AGREEMENT

This Texas Data Privacy Agreement ("DPA") is entered into by and between the Wichita Falls Independent School District (hereinafter referred to as "LEA) and BrainPOP LLC (hereinafter referred to as "Operator"). This DPA modifies and is incorporated into the Vendor's Terms of Use and Privacy Policy as posted on www.brainpop.com as updated from time to time ("Service Agreement"). To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Service Agreement and this DPA, the DPA shall supersede.

RECITALS

WHEREAS, the Operator has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to the Service Agreement; and

WHEREAS, in order to provide the Services described in the Service Agreement, the Operator may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal 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 Operator's Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

WHEREAS, this Agreement complies with Texas and Federal laws; 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 Operator may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Texas 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.** For Operator to provide services to the LEA it may become necessary for the LEA to share certain Data related to the LEA's students, employees, business practices, and/or intellectual property. This agreement describes responsibilities to protect Data between the LEA and Operator.

2. **Nature of Services Provided.** The Operator has agreed to provide the following digital educational services as set out in the Service Agreement.

3. **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 "A"

4. **DPA Definitions**. The definitions of terms used in this DPA are found in Exhibit "B". 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. **Data Property of LEA.** All Data transmitted to the Operator pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Operator further acknowledges and agrees that all copies of such Data transmitted to the Operator, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Operator shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Data notwithstanding the above. Operator 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 Data 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. Operator shall respond in a reasonably timely manner (and no later than five (5) days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA in a reasonable time not to exceed seven (7) days, who will follow the necessary and proper procedures regarding the requested information.

3. **Access to Student Generated Content**. Operator shall, at the request of the LEA, make Pupil Generated Content available in a readily accessible format.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within one (1) business day) redirect the Third Party to request the data directly from the LEA. The parties shall promptly notify one another in advance of a compelled disclosure to a Third Party and provide a copy of the request no later than ten (10) business days before disclosure is required. The Operator will not use, disclose, compile, transfer, sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof.

   Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act (Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.

5. **No Unauthorized Use**. Operator shall not use Data for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors.** Operator shall indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting the acts of omissions of its Subprocessors/subcontractors. Operator obligations with respect to any subprocessors/subcontractors shall extend only to those

subcontractors directly in contact with the District or any school thereof, and not subcontractors providing general ancillary services, such as hosting services. The indemnities set forth herein shall be limited to the amounts covered by insurance and subject to the following: LEA shall provide Operator 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 III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other applicable Federal and Texas privacy statutes and legal requirements.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 34 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, and determine whether Operator qualifies as a school official.

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

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

ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance.** The Parties expect and anticipate that Operator may receive personally identifiable information in education records from the District only as an incident of service or training that Operator provides to the LEA pursuant to this Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes quoted in this DPA. The Parties agree that Operator is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records.

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. Operator also acknowledges and agrees that it shall not make any re-disclosure of any Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Data, without the express written consent of the LEA.

3. **Employee Obligation.** Operator shall require all its employees, agents, and Subprocessors (if any) who have access to Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Operator agrees to require and

maintain an appropriate confidentiality agreement from each of its employees, agents, or Subprocessors (if any) with access to Data pursuant to the Service Agreement.

4. **No Disclosure.** De-identified information may be used by the Operator 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). Operator agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Operator shall dispose of or delete all Data obtained under the Service Agreement in accordance with the Service Agreement. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. The duty to dispose of Data shall not extend to data that has been de-identified or otherwise downloaded or transferred by the LEA or an authorized user, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Data" Form, a copy of which is attached hereto as Exhibit "C"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within three (3) calendar days of receipt of said request.

6. **Advertising Prohibition.** Operator is prohibited from using or selling Data to (a) market or advertise to the LEA's students, families/guardians, or the LEA's employees; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by an Operator; (c) develop a profile of a student, family member/guardian or group, or an LEA employee for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations unless the LEA has provided written notice to the Operator to cease such personalized learning recommendations.

7. **Access to Data.** Operator shall make Data in the possession of the Operator available to the LEA immediately (not to exceed one (1) business day) upon request by the LEA.

ARTICLE V: DATA PROVISIONS

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

   a. **Passwords and Employee Access.** Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level suggested by Article 4.3 of NIST 800-63-3. Operator shall only provide access to Data to employees or contractors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.

b. **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. Operator 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.

c. **Employee Training.** The Operator shall provide periodic security training to those of its employees who operate or have access to the system. Further, Operator shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

d. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

e. **Security Coordinator.** Operator shall provide the name and contact information of Operator's Security Coordinator for the Data received pursuant to the Service Agreement, pursuant to Exhibit D.

f. **Subprocessors Bound.** Operator shall enter into written agreements whereby Subprocessors agree to secure and protect Data in a manner consistent with the terms of this Article V. Operator shall periodically conduct or review compliance monitoring and/or assessments of Subprocessors to determine their compliance with this Article.

g. **Periodic Risk Assessment.** Operator further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA with the results of the above risk assessments and will promptly modify its security measures as needed based on those results in order to meet its obligations under this DPA.

h. **Backups.** Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of Data or any portion thereof.

i. **Audits.** Upon receipt of a request from the LEA, the Operator will allow the LEA to audit compliance with this DPA. The LEA's right to audit shall only apply to Operator's books, records and documents that are directly related to the LEA or to the District and number of audits shall be limited to no more than one (1) audit per year.

j. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any agency audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA.

U?

    k. Data Transfer. Operator agrees that all data will be transferred using secure FTP and/or physical delivery, at the LEA's discretion.

2. **Data Breach.** When Operator reasonably suspects and/or becomes aware of a disclosure or security breach concerning any Data covered by this Agreement, Operator shall timely notify the District and take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible.

    a. Subject to the following requirements, the Operator shall provide a security breach notification to the LEA.

        i. 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.

        ii. The security breach notification described above in section 2(a)(i) shall include, at a minimum, the following information:

            1. The name and contact information of the reporting LEA subject to this section.
            2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
            3. 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.
            4. 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.
            5. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

        iii. The security breach notification must include at least:
            1. Information about what the Operator has done to protect individuals whose information has been breached.
            2. Advice on steps that the person whose information has been breached may take to protect himself or herself.
            3. Information about the steps the Operator has taken to cure the breach and the estimated timeframe for such cure.

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

    c. Operator further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of 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.

    d. In the event of a data breach, Contractor will assist the LEA in contacting and informing any parties, including students, parents and legal guardians which may have been affected by the security incident.

    e. The Parties agree that any breach of the privacy and/or confidentiality obligation set forth in the DPA may, at the LEA's discretion, result in the LEA immediately terminating the Service Agreement and any other agreement for goods and services with Operator. Termination does not absolve the Operator's responsibility to comply with the disposition procedures of Data.

    f. Operator shall timely notify law enforcement as appropriate of any breach or suspected breach.

3. **Data "As-is."** Operator agrees and understands that the LEA will provide data to the Operator "as is" and "as available." The LEA is not under any obligation to modify the data, including but not limited to creating any different student identification numbers or alias.

ARTICLE VI: MISCELLANEOUS

1. **Term.** The Operator shall be bound by this DPA for the duration of the Service Agreement or so long as the Operator maintains any Data, whichever is later. Notwithstanding the foregoing, Operator 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 Operator shall dispose of all of LEA's Data pursuant to Article IV, section 5.

4. **Priority of Agreements.** This DPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other 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 or first class mail, postage prepaid, sent to the designated representatives and at the address provided below:

The designated representative and mailing address for the Operator for this Agreement is:

Name:_ Legal Department_____
Position:_____
Mailing Address:_____ BrainPOP LLC_____
_____ 71 W 23rd St., 17th Floor, New York, NY 10010_____

The designated representative and mailing address for the LEA for this Agreement is:

Name: Timothy Sherrod
Position: Chief Financial Officer
Mailing Address: Wichita Falls ISD
1104 Broad
Wichita Falls, Texas 76301

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of an authorized representative from 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 TEXAS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

    Notwithstanding the foregoing, any claim in connection with this Service 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. The ELA shall not file any such legal action until 10 days after such notification.

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

10. **Waiver.** Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.

11. **Assignment.** None of the parties to this DPA may assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of an authorized representative of the other party to this DPA. Notwithstanding the foregoing or anything to the contrary in this Agreement, Operator shall have the right without consent to assign this Service Agreement or rights hereunder or delegate obligations (a) to any affiliate of Operator, or (b) to any third party that has acquired all or substantially all of its assets or business, whether by merger, acquisition, transfer, reorganization or otherwise; provided that any such assignment or delegation to any affiliate or third party acquirer is conditioned upon assignee's assumption of all obligations and liabilities of the Operator hereunder.

ARTICLE VII: MISCELLANEOUS PROVISIONS

12. **Venue.** Both parties agree that venue for any litigation arising from this contract shall lie in state or federal court having jurisdiction over Travis County, Texas.

13. **Notifications of Amendments to Policy.** Operator shall not change how Data is collected, used, or shared under the terms of the DPA and corresponding Service Agreement in any way without advance notice to and written consent by an authorized representative of the LEA. Operator shall provide notice to the LEA of any proposed change to its Terms of Use, Privacy Policy, and/or any similar policies/procedures thirty (30) days prior to the implementation of any such change. This agreement supersedes online Terms of Use and Conditions.

14. **Severability.** The provisions of this DPA are severable. If a court of competent jurisdiction determines that any portion of this DPA is invalid or unenforceable, the court's ruling will not affect the validity or enforceability of the other provisions of the DPA.

15. **Insurance.** Operator shall take out and maintain, at its expense, until termination of the Service Agreement, at least the following insurance with an appropriately licensed insurance company in the state of Texas:

Insurance Type	Amount Required
Commercial General Liability	$1,000,000
BI & PD - each occurrence	$ 100,000
BI & PD – aggregate	$ 300,000
Medical Expenses – any one person	$ 10,000
Personal & Adv Injury – each occurrence	$1,000,000
Commercial Auto Liability	$1,000,000
-- All owned/non-owned/hired combined single limits	
Excess/Umbrella Liability	$10,000,000
Workers' Compensation	Statutory Limits

| Errors & Omissions Coverage | $2,000,000 |
| Cyber Liability Coverage | $2,000,000 |

Operator represents that it is not an employee of the LEA and that it has or will follow applicable Texas statutory guidelines regarding workers compensation. Operator shall require all subcontractors performing any work on site of the District to maintain coverage as specified herein.

16. **Data Storage.** Operator acknowledges and agrees that all electronic data and records will not be shipped, stored, transferred, or exported outside the United States, including any backups or copies, without prior written consent from an authorized representative of the LEA.

17. **Notification of Criminal History.** A person or business entity that enters into a contract with a Texas public school district, such as the LEA, must give advance notice to the LEA if the person or an owner or operator of the business entity has been convicted of a felony. Pursuant to the Texas Education Code §22.0834 and the Texas Government Code §411.082, Operator will, at least annually, obtain criminal history record information that relates to an employee, applicant, or agent of Operator, if the person has or will have continuing duties related to the LEA, and the duties are or will be performed on the LEA's property or at another location where students are regularly present. Operator shall assume all expenses associated with the background checks, and shall immediately remove any employee or agent who was convicted of a felony or a misdemeanor involving moral turpitude from the LEA's property or other location where students are regularly present. Licensee shall determine what constitutes "moral turpitude" or "a location where students are regularly present." Operator understands that failure to comply with the requirements of this section may be grounds for termination of the Service Agreement.

Operator further agrees that employees who will have access to raw data that has not been disaggregated will also undergo criminal background checks at least annually. Operator shall assume all expenses associated with the background checks, and shall immediately remove any employee or agent who was convicted of a felony or a misdemeanor involving moral turpitude from the LEA's property or other location where students are regularly present.

18. **Compliance with Texas Government Code Chapter 2270; Prohibition on Contract with Companies that Boycott Israel.** Operator represents and warrants that it does not boycott Israel and will not boycott Israel during the Term of the Service Agreement.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Texas Data Privacy Agreement as of the date of the last signature noted below.

Authorized Representative of LEA:

BY:_____ Date:___11/22/2019_____

Printed Name:__Timothy Sherrod_____ Title/Position:_____Chief Financial Officer__

Authorized Representative of Operator:

BY:_____*H. Scott Kirkpatrick*_____ Date:_____11/22/19_____

Printed Name:__H. Scott Kirkpatrick___ Title/Position:_Chief Executive Officer__

EXHIBIT "A"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	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: Teacher page events, i.e. "the teacher saw X movie 3 times"	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communication that are captured (emails, blogs 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)	
Enrollment	Student school enrollment	
	Student grade level	X

Category of Data	Elements	Check if used by your system
	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	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialized education services (IEP/504)	
	Living situations (homeless/foster care)	
	Other indicator information- Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student	Local (school	

Category of Data	Elements	Check if used by your system
Identifiers	district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	X
	Student app passwords	X
Student Name	First and/or last	X
Student In App Performance	Program/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

Category of Data	Elements	Check if used by your system
	Other student work data – Please specify: See Exhibit D "other"	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data –Please specify:	
Transportation	Student bus assignment	
	Student pick-up/drop off location	
	Student bus card ID	
	Other transportation data-Please specify:	
Other	Please list each additional data element used, stored or collected through the services as defined in Exhibit A: See Exhibit D "other"	X

<center>

EXHIBIT "B"
DEFINITIONS

</center>

HB 2087: The statutory designation for what is now Texas Education Code Texas Education Code Chapter 32 relating to pupil records.

Data: Data shall include, but is not limited to, the following: student data, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Operator's services.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Data.

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

Data Destruction: Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.
NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 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. This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator 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 Data.

Pupil-Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

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

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

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

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

Texas Student Privacy Alliance: The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

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

EXHIBIT "C"

DIRECTIVE FOR DISPOSITION OF DATA

Wishita Falls ISD directs BrainPOP LLC to dispose of data obtained by Company pursuant to the terms of the Service Agreement between LEA and Company. The terms of the Disposition are set forth below:

1. Extent of Disposition

   _____ Disposition is partial, The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

   [Insert categories of data here]

   _____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

   _____ Disposition shall be by destruction or deletion of data.

   _____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

   [Insert or attach special instructions.]

3. Timing of Disposition

   Data shall be disposed of by the following date:

   _____ As soon as commercially practicable

   _____ By (Insert Date]

4. Signature

   _____   _____
   Authorized Representative of LEA   Date

5. Verification of Disposition of Data

   _____   _____
   Authorized Representative of Company   Date

Exhibit D – "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.