# NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT VERSION (2019)

**Oyster River Cooperative School District**

**and**

**BrainPOP LLC**

**November 22, 2019**

This New Hampshire Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Oyster River Cooperative School District (hereinafter referred to as "LEA") and BrainPOP LLC (hereinafter referred to as "Provider") on November 22, 2019. The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS,** the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

**WHEREAS**, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in New Hampshire the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

**WHEREAS**, the use of Contractor's products shall be governed by the Terms of Use and Privacy Policy as posted on www.brainpop.com and as updated from time to time ("Terms of Use"), except in the case of a conflict with this DPA, in which case the DPA will govern; and

**WHEREAS,** in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that may be covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 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; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

**WHEREAS,** the documents and data transferred from New Hampshire LEAs and created by the Provider's Services are also subject to several New Hampshire student privacy laws, including RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS,** the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the applicable privacy laws referred to above and to establish implementing procedures and duties.

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

## ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, SOPIPA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described in Exhibit "A".

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described 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". In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other personally identifiable Pupil Records transmitted to the Provider pursuant to this Agreement and Terms of Use is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and applicable state law, 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. The Provider will cooperate and provide Student Data notwithstanding the above.

2. **Parent Access**. LEA shall establish reasonable procedures by which aparent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the export of pupil-generated content, consistent with the functionality of services. Parents can request login information from the student or teacher to access their student's records. Parents can also request that the administrator on the account appointed by the District correct any erroneous information. Provider shall cooperate and respond within fourteen days (14)(14to the LEA's request for personally identifiable information in a Pupil's Records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review, delete, or amend any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. LEA may export Student Data by using the administrator dashboard in the individual account system at any time.

4. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, 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 and shall cooperate with the LEA to collect the required information unless otherwise provided by law. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student 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 Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. 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.

5. **No Unauthorized Use**. Provider shall not use Student Data or personally identifiable information in a Pupil Record for any purpose other than as explicitly specified in this DPA. Provider may provide Personally Identifiable Information to partners, business affiliates, and third party service providers who work for Provider 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 information solely as it pertains to the provision of the LEA's services. They do not have the independent right to share personally identifiable information. Provider may share anonymous or de-identified information about users when it is using third party web analytical tools, for tracking analytical information. Provider may use or share anonymous or aggregate and de-identified information to evaluate, inform, or show the efficacy of its services.

6. **Subcontractors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect the confidentiality of Student Data. The Provider will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors that cause the Provider to breach any of the Provider's obligations under this DPA.

## ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. If applicable, LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

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

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

## ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above, if applicable. Provider also acknowledges and agrees that it shall not make any re-disclosure of any personally identifiable Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it is necessary to share with subprocessors in order to provide the services or fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data.

4. **No Disclosure**. De-identified or anonymous information, as defined in Exhibit "C", 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 the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA and Terms of Use. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

5. **Disposition of Data.** Districts and schools are able to download or delete information at any time and in real time using the administrator dashboard. Once information is deleted, Provider does not retain any copies. If information was not deleted by the school or the district before the subscription expired, Provider retains such information for a limited period of thirty days. Student accounts within My BrainPOP classrooms that have not been active for a period of two years are automatically deleted as well. After such a period, all information is automatically disposed of and deleted - first from our server and then, two weeks later, from any back-up server. At that point it cannot be restored. If the District's jurisdiction requires the deletion of student data within a shorter time period, or upon immediate termination of the subscription, LEA is required to delete such data using the administrator dashboard as mentioned above or contact us for assistance. Districts and schools may request copies of any raw data from the database, which shall be provided within ten days of the request.

6. **Advertising Prohibition**. Provider is prohibited from leasing, renting, 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 products; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the products.

## ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology 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" 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 a level suggested but not required by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements. All employees with access to Student Records shall pass criminal background checks.

    b. **Destruction of Data**. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA as outlined in Article V, Section 5.

    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 DPA in a secure computer environment and

not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

d. **Employee Training**. The Provider shall provide recurring, periodic (no less than annual, with additional sessions if needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider's business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, LEA may contact legal@brainpop.com if there are any security concerns or questions.

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

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

g. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

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

i. **Audits.** Upon receipt of a request from the LEA, no more than once per year, except in the case of a breach, the Provider will allow the LEA to audit documents and records directly related to the LEA to the extent such audit does not compromise other customers. Provider may provide an independent, third-party report in place of allowing the LEA to conduct the audit, if the LEA consents to the independent, third-party. The LEA may not unreasonably withhold its consent.

The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA and provide access to records pertaining directly related to the Provider, LEA and delivery of Services to the

Provider LEA's Student Data. Failure to cooperate shall be deemed a material breach of the Agreement.

**j. New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education. Specifically, the Provider agrees to:

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10) Perform maintenance on organizational systems;

(11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student Data and maintain accountability for media during transport outside of controlled areas;

(16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19) Protect the confidentiality of Student Data at rest;

(20) Identify, report, and correct system flaws in a timely manner;

(21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22) Monitor system security alerts and advisories and take action in response; and

(23) Update malicious code protection mechanisms when new releases are available.

i. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA promptly after 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," "When it Occurred," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

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

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

      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

vi. The estimated number of students and teachers affected by the breach, if any.

c. If applicable, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.

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

d. Provider agrees to adhere to all applicable requirements in the New Hampshire Data Breach law and in applicable 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 to LEA 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.

## ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent as long as the subscription has been terminated or expired.

   The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival**. If the subscription is terminated or expired, LEA will delete the data, otherwise the data will be retained for a period of 30 days following termination of the subscription.

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to

comply with the privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100, to the extent applicable. In the event there is conflict between the terms of the DPA and the Terms of Use or any other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

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

   The designated representative for the Provider for this Agreement is:

Name Legal Department _____
Title _____
Address ___71 W 23rd St 17th Floor New York NY 10010
_____
Telephone ____212-574-6000_____
Email
legal@brainpop.com_____

The designated representative for the LEA for this Agreement is:

Joshua Olstad
IT Director, Oyster River Cooperative Schools
36 Coe Drive, Durham, NH 03824
603-389-3299
jolstad@orcsd.org

6. **Entire Agreement**. This DPA and the Terms of Use 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 NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF STRAFFORD COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY. Without derogating from the above, any claim that LEA may have must first, and before taking any other legal action, be submitted to the Service Provider in the form of a complaint (to: info@brainpop.com), to enable the parties to resolve the claim in a friendly and effective manner. If the parties fail to resolve the claim in this manner in a reasonable timetable, it shall be resolved in the exclusive jurisdiction and venue as specified above. Notwithstanding the foregoing, the Service Provider 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 Agreement, 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.

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. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart.

## ARTICLE VII- GENERAL OFFER OF 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 to any other school district who signs the acceptance in said Exhibit.

[*Signature Page Follows*]

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

OYSTER RIVER COOPERATIVE SCHOOL DISTRICT

By: Joshua Olstad (Nov 26, 2019) Date: 11/26/2019

Printed Name: Joshua Olstad Title/Position: IT Director

BRAINPOP LLC

By: H. Scott Kirkpatrick Date: 11/22/19

Printed Name: H. Scott Kirkpatrick Title/Position: Chief Executive Officer

## EXHIBIT "A"

DESCRIPTION OF SERVICES

Subscription to online education content:

BrainPOP

BrainPOP Jr.

BrainPOP ELL

BrainPOP Español

BrainPOP Français

BrainPOP Educators

# EXHIBIT "B"

## SCHEDULE OF DATA

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Application Technology Meta Data | IP Addresses of users, Use of cookies etc. | 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: | |
| 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 | |
| | | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Schedule | Student scheduled courses | |
| | Teacher names | x |
| | | |
| Special Indicator | English language learner information | |
| | Low income status | |
| | Medical alerts | |
| | 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 | |
| | 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. | |
| | Other student work data - Please specify: | x |
| | | |
| Transcript | Student course grades | |
| | Student course data | |

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

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| | Other transportation data - Please specify: | |
| | | |
| Other | Please list each additional data element used, stored or collected by your application | x |

## 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

**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. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

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

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

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

Place of birth Social Media Address
Unique pupil identifier
Credit card account number, insurance account number, and financial services account number
Name of the student's parents or other family members

General Categories:

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

Information in the Student's Educational Record

Information in the Student's Email

**Provider:** For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

**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 personally identifiable information that directly relates to a pupil that is maintained by LEA and (2) any personally identifiable information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

**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. The definition of "school official" encompasses the definition of "authorized school personnel" under 603 CMR 23.02.

**Student Data:** Student Data includes any personally identifiable 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, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, 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 New Hampshire and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the

Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**Subscribing LEA**: An LEA that was not party to Terms of Use.

**Subprocessor:** For the purposes of this Agreement, the term the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms. "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 direct 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 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 an entity that is not the provider or LEA.

## EXHIBIT "D"

## DIRECTIVE FOR DISPOSITION OF DATA

**Omitted on Purpose**

## OPTIONAL: EXHIBIT "F"

## DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? □ Yes □ No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002

____ CIS Critical Security Controls

____ NIST Framework for Improving Critical Infrastructure Security

____ Other: _____

j. Does your organization store any customer data outside the United States? □ Yes □ No

k. Does your organization encrypt customer data both in transit and at rest? □ Yes □ No

l. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: _____

Contact information: _____

m. Please provide any additional information that you desire.