BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	**BrainPOP LLC**
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary ☐IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.
Description of the purpose(s) for which Contractor will receive/access PII	The exclusive purposes for which personally identifiable data as defined in Education Law Section 2-D will be used by Contractor are limited to the purposes to provide the online educational content service according to Contractor's practices as outlined in its Terms of Use and Privacy Policy. Contractor does not sell student data.
Type of PII that Contractor will receive/access	Check all that apply: ☒Student PII ☐APPR PII

Contract Term	Contract Start Date 7/1/2023 Contract End Date 6/30/2024
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☒ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors. BrainPOP does not utilize third party subcontractors to directly provide Services to EA.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: ~~• Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.~~ • Securely delete and destroy data. The agreement expires when the subscription period ends or the subscription is terminated. EA is able to delete student personally identifiable information at any time and in real time using the Administrator dashboard. Once that information is deleted, it is deleted from our servers – first from our servers and then, after two weeks later, from any back-up server. If information was not deleted by EA before the subscription expired, we retain such information for a limited period of two years after expiration.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request. The accuracy of personally identifiable information may be challenged by contacting the West Suffolk Data Privacy Officer or BrainPOP at privacy@brainpop.com.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒Using a cloud or infrastructure owned and hosted by a third party. ☐Using Contractor owned and hosted solution ☐Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: The data is stored domestically at a physically secure location. Access is only granted to those employees directly involved in maintaining server integrity. Employees receive privacy training on a yearly basis and some receive specialized training whenever policies or obligations change.
Encryption	Data will be encrypted while in motion and at rest. Data is protected both at rest and in motion as described in the Privacy Policy. Contractor has industry standard password protections, administrative procedures, encryption, and firewalls in place.

Western Suffolk BOCES - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state**. While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	BrainPOP employs administrative, physical, and technical measures in accordance with industry standards to protect data by implementing physical and technical safeguards, firewalls, security monitoring, restriction of system access to only authorized personnel, encryption, etc.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	BrainPOP employs administrative, physical, and technical measures in accordance with industry standards to protect data by implementing physical and technical safeguards, firewalls, security monitoring, restriction of system access to only authorized personnel, encryption, etc.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Personnel with access to Student Records pass criminal background checks and undergo periodic privacy training on annual basis.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Contractor's employees enter into an employment agreement that outlines non-disclosure, data security, privacy obligations. Contractor may provide Personally Identifiable Information to its partners, business affiliates, and third party service providers who work for Contractor and operate some of its functionalities such as hosting, streaming, credit card processing services and marketing. Contractor's third party service providers are bound contractually to practice commercially reasonable security measures and to use your Personally Identifiable Information solely as it pertains to the provision of their services.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	In the event of unauthorized access to Personally Identifiable Information, we will notify the affected subscriber(s) in accordance with applicable law, and as appropriate, coordinate with the subscriber to support notification of affected individuals, students, and families.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Each school or district Administrator has access to a dashboard that allows them to create, update, review, modify and delete individual accounts, and monitor logins within the individual accounts. EA is able to delete student personally identifiable information at any time and in real time using the Administrator dashboard. EA may request copies of their student personal information (which includes an CSV template file of names, classes and quiz scores), which shall be provided within four (4) weeks of the written request.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Secure data destruction is available through Administrator dashboard or by submitting a written request (to : privacy@brainpop.com). Once that information is deleted, it is deleted from our servers – first from our servers and then, after two weeks later, from any back-up server.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor's data security and privacy programs aligns with industry reasonable standard. For more information, please see BrainPOP Privacy Policy posted at www.brainpop.com.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Contractor's data security and privacy programs aligns with industry reasonable standard. For more information, please see BrainPOP Privacy Policy posted at www.brainpop.com.

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org . (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	*Anna Friedman*
[Printed Name]	Anna Friedman
[Title]	Sr. Director, Legal
Date:	6/7/2023