

CONFIDENTIALITY
AND
DATA SECURITY AND PRIVACY
STANDARDS AGREEMENT

This Agreement made this 3 day of August, 2022 by and between Lexia Learning Systems LLC (“VENDOR”) having its principal place of business at 300 Baker Avenue, Suite 320, Concord, MA 01742, and GREAT NECK UNION FREE SCHOOL DISTRICT (the “SCHOOL DISTRICT”), having its principal place of business at 345 Lakeville Road, Great Neck, NY 11020.

WHEREAS, the Vendor will receive “student data” as that term is defined in New York Education Law section 2-d and the regulations promulgated thereunder (together, “Educ. Law §2-d”); and

WHEREAS, both the School District and Vendor are desirous of fulfilling their respective obligations under Educ. Law §2-d and the regulations promulgated thereunder.

NOW THEREFORE, in consideration of the mutual promises and covenants contained in the Agreement, the parties hereto mutually agree as follows:

1. VENDOR, its employees, and/or agents agree that all information obtained in connection with the services provided for in this Agreement is deemed confidential information. VENDOR, its employees, and/or agents shall not use, publish, discuss, disclose or communicate the contents of such information, directly or indirectly with third parties, except as provided for in this Agreement. VENDOR further agrees that any information received by VENDOR, its employees, and/or agents during the course of the services provided pursuant to this Agreement which concerns the personal, financial, or other affairs of SCHOOL DISTRICT, its employees, agents, clients, and/or students will be treated by VENDOR, its employees, and/or agents in full confidence and will not be revealed to any other persons, firms, or organizations.

2. VENDOR acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by Educ. Law §2-d, from records maintained by SCHOOL DISTRICT that directly relate to a student(s) (hereinafter referred to as “education record”). VENDOR understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it shall:

- a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
- b. not use the education records for any purposes other than those explicitly authorized in this Agreement;

c. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

d. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5 and the National Institute of Standards and Technology Cyber Security Framework Version 1.1.

3. VENDOR further understands and agrees that it is responsible for submitting a data security and privacy plan to SCHOOL DISTRICT prior to the start of the term of this Agreement. Such plan shall outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with SCHOOL DISTRICT's policy on data security and privacy, as adopted. Further, such plan shall include a signed copy of SCHOOL DISTRICT's Parents' Bill of Rights and the training requirement established by VENDOR for all employees who will receive personally identifiable information from student records (hereinafter referred to as "student data").

4. VENDOR understands that as part of SCHOOL DISTRICT's obligations under Educ. Law §2-d, VENDOR is responsible for providing SCHOOL DISTRICT with supplemental information to be included in SCHOOL DISTRICT's Parents' Bill of Rights. Such supplemental information shall be provided to SCHOOL DISTRICT within ten (10) days of execution of this Agreement and shall include:

a. the exclusive purposes for which the student data will be used;

b. how VENDOR will ensure that subcontractors, persons or entities that VENDOR will share the student data with, if any, will abide by data protection and security requirements;

c. that student data will be returned or destroyed upon expiration of the Agreement;

d. if and how a parent, student, or eligible student may challenge the accuracy of the student data that is collected; and

e. where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

5. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data, VENDOR shall immediately notify SCHOOL DISTRICT and advise it as to the nature of the breach and steps VENDOR has taken to minimize said breach. Said notification must be made within seven (7) days of the breach. In the case of required notification to a parent or eligible student, VENDOR shall promptly reimburse SCHOOL DISTRICT for the full cost of such notification.

6. In the event that VENDOR fails to notify SCHOOL DISTRICT of a breach, said failure shall be punishable by a civil penalty of the greater of \$5,000 or up to \$20 per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law, section 899-aa(6)(a).

7. Except as set forth in paragraph (f) above, in the event VENDOR violates Education Law 2-d, said violation shall be punishable by a civil penalty of up to \$1,000. A second violation involving the same data shall be punishable by a civil penalty of up to \$5,000. Any subsequent violation involving the same data shall be punishable by a civil penalty of up to \$10,000. Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law section 899-aa(6)(a).

8. VENDOR shall indemnify and hold SCHOOL DISTRICT harmless from any claims arising from its breach of the within confidentiality and data security and privacy standards provision.

Upon termination of this Agreement, VENDOR shall return or destroy all confidential information obtained in connection with the services provided herein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this agreement the day and year first above written.

GREAT NECK UNION FREE SCHOOL
DISTRICT

Date: 8/31/22

By: *Joseph Cangialosi*

Lexia Learning Systems
LLC Date: 16-Sep-2022

By:

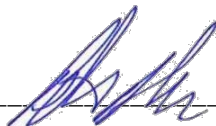
Peter Koso
Peter Koso, Vice President

Parents' Bill of Rights for Data Privacy and Security

The Great Neck Union Free School District is committed to protecting the privacy and security of each and every student's data. Parents should be aware of the following rights they have concerning their child's data:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. The confidentiality of a student's personally identifiable information is protected by existing state and federal laws, and safeguards such as encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third party contractors are required to employ technology, safeguards and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.
4. A complete list of all student data elements collected by the State Education Department is available for public review at: <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to file complaints about possible breaches of student data. Parents may submit a complaint regarding a potential breach by the District to the Superintendent of Schools, 345 Lakeville Road, Great Neck, New York 11020. The School District shall promptly acknowledge any complaints received and commence an investigation into the complaint, while taking the necessary precautions to protect personally identifiable information. The School District shall provide a response detailing its findings from the investigation no more than sixty (60) days after receipt of the complaint. Complaints pertaining to the State Education Department or one of its third party vendors should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, or email to privacy@nysed.gov.
6. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.
7. If the District enters into a contract with a third party in which student, teacher, or principal data is shared with a third party, supplemental information for each such contract will be appended to this Parents' Bill of Rights.
8. Parents may access the State Education Department's Parents' Bill of Rights at: http://www.nysed.gov/common/nysed/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Acknowledged by: _____



[Lexia Learning Systems LLC](#) 16-Sep-2022
Organization Date

Data Security and Privacy Plan

As per the Agreement between the undersigned and the School District, this plan must be completed by the Service Provider within 10 days of execution of the Agreement.

1. Describe how you will implement applicable data security and privacy contract requirements over the life of the contract.

Lexia shall limit access to protected data to those of its employees, agents and contractors that need to receive such information to enable Lexia to provision and support its services to its school and district customers and who have received data protection training and are under contractual obligations of confidentiality to Lexia with respect to such information no less restrictive than those herein, and for whom Lexia shall remain liable. Lexia shall ensure, to the extent that it comes into possession of student data and/or teacher or principal data pursuant to the Agreement, that it will not otherwise share such protected data with any additional parties, including any unauthorized subcontractor or non-employee agent, without prior written consent of the district.

Initial

2. Exclusive Purposes for Data Use

- a. Please list the exclusive purposes for which the student data [or teacher or principal data] will be used by the service provider include.

Initial

For the operation of the Lexia Software-as-a-Service (SaaS) products.
Lexia Application License:
<https://www.lexialearning.com/privacy/eula>
Lexia Application Data Privacy Policy
<https://legal.lexialearning.com/legal/application-privacy.html>
Lexia Student Records Privacy Statement and Security Plan:
<https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan>

3. Data Accuracy/Correction Practices

- a. Parent [student, eligible student, teacher or principal] may challenge the accuracy of the data by...

Parents, students, or guardians should contact the District with any concerns. Lexia will work with the District to correct any errors.

Initial

4. Subcontractor Oversight Details

- a. This contract has subcontractors: Yes _____ No X
- b. Describe how the contractor will ensure subcontractors abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations:

Should this arise, by contractual obligation.

Initial ML

5. Security Practices

- a. Where is the data stored? (described in such a manner as to protect data security)
Data is stored in a USA-based Tier 1 facility.
- b. The security protection practices taken to ensure data will be protected include:

Best industry practices for physical and logical access controls.
Data is encrypted in transit and at rest.

Initial ML

6. Contract Lifecycle Practices

- a. The agreement expires per applicable Lexia Quotes (upon deactivation of the licenses).
- b. When the agreement expires,
 - i. How long is the student data [or teacher or principal data] retained?
Until the agreement expires.
 - ii. How is the student data disposed? Data is securely deleted from the production database and any backups.

Initial ML

7. Encryption Practices

- a. Data encryption is applied in accordance with Education Law 2-d 5(f)(5)

Yes No

Initial ML

8. Training Practices


- a. Annual training on federal and state law governing confidentiality is provided for all officers, employees, or assignees who have access to student [or teacher or principal data]

Yes No

Initial ML

Lexia Learning Systems LLC
Company Name

Peter Koso, Vice President
Print Name and Title



Signature of Provider

16-Sep-2022
Date