RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Lexia Learning Systems LLC ("Service Provider") on 01/23/2020 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ◉ No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ◉ No ○

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ◉ No ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes (●) No ( )

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes (●) No ( )

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes (●) No ( )

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes (●) No ( )

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes (●) No ( )

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes (●) No ( )

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes (●) No ( )

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes (●) No ( )

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes (●) No ( )

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes (●) No ( )

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes (●) No ( )

3. Vendors cannot sell student information.

   Agree: Yes (●) No ( )

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes (●) No ( )

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes (●) No ( )

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes (●) No ( )

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes (●) No ( )

As an authorized representative of my organization, I accept the conditions listed in this document.

Peter Koso, Vice President
Print Name

Signature, Date

Laura Assem, 01/30/2020
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section 1.6: External Security

Lexia uses Amazon Web Services for its server infrastructure and content delivery.
Lexia servers are located in a Tier 1 facility. Physical security and access is provided by a system of access cards, biometric readers, keys, and additional physical controls. A security guard is on duty 24x7. Please refer to https://aws.amazon.com/compliance/data-center/data-centers/ for additional information. Access to Lexia systems is limited to a subset of Lexia IT personnel, all of whom have undergone background checks.
Within the AWS infrastructure Lexia maintains redundant firewalls, network switches, and load balancers.
Our server, API, and authentication tiers utilize load balancers and redundant servers to provide high availability. The Lexia database tier is also redundant with a primary and multiple reader copies maintained in real-time across multiple availability zones within AWS. Daily encrypted database backups are maintained for 7 days. The Lexia application configuration and architecture is designed to provide redundancy to appropriately protect against risk of loss and enable customer data restoration.

Section 1.7: Internal Security

District data is accessed by Lexia employees with a need-to-know, for example, Customer Support engineers, Development, Quality Assurance, and Research to address problems or provide customer-requested support services or improve the customer experience. All Lexia employees undergo a criminal background check annually. All Lexia employees are required to take data privacy training.
In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.
We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length, and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.
Student data is retained for the duration of the contract to the district. Within 45 days following expiration or termination, and as directed in writing by the District account administrator, we start the process of removing and destroying student personally identifiable data in our possession. The designated District account administrator will receive a series of notifications from us

Section II.2: Exporting of Student-Created Content

N/A. There is no student-created content.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Individual student users cannot access or delete data. The District Administrator for the Lexia account can delete students and student data through the myLexia administrator dashboard within the program. If a parent, legal guardian or student contacts us with a request to review the user's Student Records or correct erroneous information, or if an agency, court, law enforcement or other entity contacts us and requests access to Student Records, we will (unless prohibited by writ or compulsory legal process) promptly notify an authorized representative of the applicable Education Client and use reasonable and good faith efforts to assist the Education Client in fulfilling such requests, as required by law and directed by the Education Client.

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Lexia Application End User License Agreement: http://www.lexialearning.com/download
Lexia Application Data Privacy Policy
http://www.lexialearning.com/privacypolicy/index.html
Lexia Student Records Privacy & Security Plan
https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan
In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.
We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.

Section II.6: Disclosure Notification

In the event of a data security breach, the affected customer(s)'s administrator-of-record will be notified within a reasonable timeframe once the breach has been identified and analyzed.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Lexia is FERPA compliant.
https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan

Section III.5: How Student Data is Protected:

Student Records Privacy Statement & Security Plan
https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan
In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.
We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.

ATTACHMENT for Item #I-6

EXTERNAL SECURITY: Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

Lexia uses Amazon Web Services for its server infrastructure and content delivery. Lexia servers are located in a Tier 1 facility. Physical security and access is provided by a system of access cards, biometric readers, keys, and additional physical controls. A security guard is on duty 24x7. Please refer to https://aws.amazon.com/compliance/data-center/data-centers/ for additional information. Access to Lexia systems is limited to a subset of Lexia IT personnel, all of whom have undergone background checks.

Within the AWS infrastructure Lexia maintains redundant firewalls, network switches, and load balancers.

Our server, API, and authentication tiers utilize load balancers and redundant servers to provide high availability. The Lexia database tier is also redundant with a primary and multiple reader copies maintained in real-time across multiple availability zones within AWS. Daily encrypted database backups are maintained for 7 days. The Lexia application configuration and architecture is designed to provide redundancy to appropriately protect against risk of loss and enable customer data restoration.

ATTACHMENT for Item #I-7

INTERNAL SECURITY: Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

District data is accessed by Lexia employees with a need-to-know, for example, Customer Support engineers, Development, Quality Assurance, and Research to address problems or provide customer-requested support services or improve the customer experience. All Lexia employees undergo a criminal background check annually. All Lexia employees are required to take data privacy training.

In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.

We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length, and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.

Student data is retained for the duration of the contract to the district. Within 45 days following expiration or termination, and as directed in writing by the District account administrator, we start the process of removing and destroying student personally identifiable data in our possession. The designated District account administrator will receive a series of notifications from us following expiration, indicating that student information has been scheduled for removal.

ATTACHMENT for Item #I-8

DISTRICT ACCESS: Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

Lexia's automated data exports contain detailed student usage and progress data that can be used to integrate with a school's data warehouse for integration with a school's dashboard.

Lexia provides detailed student-level information around usage, skills, and progress data via our automated and manual exports. In addition, most of the online reports contain the ability to export the raw data behind the report into a spreadsheet. Lexia's automated data export feature provides nightly exports of robust student usage, progress, and skills data. CSV files are generated nightly and are securely stored on a district's dedicated SFTP site.

Student data is retained for the duration of the contract to the district. Within 45 days following expiration or termination, and as directed in writing by the District account administrator, we start the process of removing and destroying student personally identifiable data in our possession. The designated District account administrator will receive a series of notifications from us following expiration, indicating that student information has been scheduled for removal.

ATTACHMENT for Item #II-2

Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

N/A. There is no student-created content.

ATTACHMENT for Item #II-4

Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

Individual student users cannot access or delete data. The District Administrator for the Lexia account can delete students and student data through the ***myLexia*** administrator dashboard within the program.

If a parent, legal guardian or student contacts us with a request to review the user's Student Records or correct erroneous information, or if an agency, court, law enforcement or other entity contacts us and requests access to Student Records, we will (unless prohibited by writ or compulsory legal process) promptly notify an authorized representative of the applicable Education Client and use reasonable and good faith efforts to assist the Education Client in fulfilling such requests, as required by law and directed by the Education Client.

ATTACHMENT for Item #II-5

Vendor will attach to this document evidence how student data is kept secure and confidential.

Lexia Application End User License Agreement:
http://www.lexialearning.com/download

Lexia Application Data Privacy Policy
http://www.lexialearning.com/privacypolicy/index.html

Lexia Student Records Privacy & Security Plan
https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan

In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.

We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.

ATTACHMENT for Item #II-6

Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

In the event of a data security breach, the affected customer(s)'s administrator-of-record will be notified within a reasonable timeframe once the breach has been identified and analyzed.

ATTACHMENT for Item #II-8

Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

Lexia is FERPA compliant.

https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan

ATTACHMENT for Item #III-5

Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Student Records Privacy Statement & Security Plan
https://www.lexialearning.com/privacy/student-records-privacy-statement-security-plan

In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.

We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.