

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Lexia Voyager Sopris Inc. ("Service Provider") on 09/09/2022 ("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

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 Please see [Section I.6: External Security](#) response below in Exhibits.
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 Please see [Section 1.7: Internal Security](#) response below in Exhibits.
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 Our online data management system allows the user incredible flexibility in generating reports, including customizing the data sets included, graphical presentation, and time periods. School and district reports can be manipulated into various types of charts (for example, bar or line graphs, etc.) to enable educators to display the data in the clearest way for the intended audience (parents, school boards, etc.).
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

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 Please see **Section II.2: Exporting of Student-Created Content** response below in Exhibits.

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 Please see **Section II.4: Review and Correcting Personally Identifiable Information (PII)** response below in Exhibits.

5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No Please see **Section II.5: Securing Student Data** response below in Exhibits.

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 Please see **Section II.6: Disclosure Notification** response below in Exhibits.

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 Please see **Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance** response below in Exhibits.

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

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 Please see **Section III.5: How Student Data is Protected** response below in Exhibits.

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.

Amy Otis

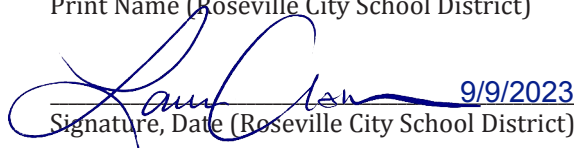
Print Name


Signature, Date

09.09.2022

Laura Assem

Print Name (Roseville City School District)


Signature, Date (Roseville City School District)

9/9/2023

EXHIBITS

Section 1.6: External Security

The Company uses market leading firewalls, routers, switches and servers to run each of its online products. These devices are constantly monitored for issues. We also apply important upgrades and patches to each device to ensure optimum and secure processing. All hardware is under warranty with the manufacturers, and we have a strict policy to replace these components at the end of their warranty periods.

Voyager Sopris solutions' application environment is segregated from the Internet through the use of a stateful firewall to ensure that access to data is protected. Firewall Ports: Voyager Sopris online applications require the use of Port 443.

Voyager Sopris manages network vulnerability by constantly scanning our network and online applications for known vulnerabilities. We use with best-of-breed vulnerability scanning and management tools, including Tenable.io and Site 24x7. We also use Netsparker and Sentinel Dynamic. We also subscribe to several security news alerts.

We notify LEAs within 72 hours after a confirmed security breach. In this case we will collaborate closely with how the district wants to handle the communication to its parents and teachers and any law enforcement agencies that need to be informed.

Section 1.7: Internal Security

Our Software Development Lifecycle Policy, approved by Cambium's Information Security Committee, defines roles and responsibilities throughout the SDLC and prohibits engineers from accessing production data except for rare and critical business needs. Exceptions to this must be for relevant and purposeful discovery, understanding and resolution of issues occurring only in the production system and not reproducible in a non-production system. Exceptions shall happen for the minimum amount of time required to understand the issue and determine an appropriate resolution and are only granted through leadership approval. Voyager Sopris environments utilize password-protected security levels to ensure that users can only access information for which each has been authorized. Sensitive data cannot be accessed by unauthorized users.

We support three different types of SIS integration to synchronize SIS data with the Voyager Sopris data management system. We offer a nightly sync option that creates a connection between the district SIS and our data management system through the transfer of a data template via SFTP. As we receive the file nightly, our system will update to align with the information in the district's SIS. Voyager Sopris has created standard file formats used for both imports and exports with a district SIS and these file formats are compatible with most standard student information systems. We partner with Clever to receive roster updates through the Clever dashboard. Voyager Sopris also supports roster integration through the standard OneRoster v1.0 initiative.

Voyager Sopris solutions' application environment is segregated from the Internet through the use of a stateful firewall to ensure that access to data is protected. Security is implemented in conjunction with the policies of our co-location facilities. The servers and the facilities they are housed in are physically secured, and network access is restricted. Physical and logical access are provided to trusted, authorized employees. Physical security measures in place at the data center include secure swipe card access and keypad access. The company applies the principle of "least privilege" throughout its entire network.

There is no separate licensing for the online data management and scoring system. All teachers who have classes, along with campus and district personnel, have access. In general, district administrators can see all information, school administrators can see all school information, and teachers can see all class information. All applications use a hierarchical access structure which limits teachers to accessing their classes, campus users to the school level, and district personnel to all schools. District-level users are created by the company. Building- and teacher-level users can be created by district-level users or by the company. Teacher-level users can be created by district- or building-level users, or by the company. Accountability, authentication, and authorization methods are in place to restrict access to utility programs that are capable of overriding our product's system and application controls.

All PII and student education data are backed up daily and retained in a secure location only accessible by authorized information technology personnel of the company. Daily backups are also kept offsite in a secure location to support the company's disaster recovery process. Voyager Sopris will delete all data upon termination of the contract, after a year of no renewals or activity, and/or at the request of the district. As database equipment is retired, it is provided to a computer recycling company, which destroys any persistent data. Our recycling company provides certificates of destruction. This data destruction is compliant with NIST 800-88.

Section II.2: Exporting of Student-Created Content

While students do not create original content in the online components of Vmath and TransMath, progress monitoring and assessment reports can be exported to personal email accounts.

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

The school district will access the solution using web browsers on both personal computers and mobile devices. This requires that each students and educator have their own license and ensures that each user/account will have data and statistics based on their usages and performance.

Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If student data is found to be inaccurate, incomplete, or out-of-date, the EA is responsible for correcting it. If you experience problems making corrections to student data, please notify us at support@voyagersopris.com or 888-399-1995 and we will assist you with making corrections.

EXHIBITS

Section II.5: Securing Student Data

We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from you. We will implement reasonable and appropriate safeguards when collecting student data from you and when storing that student data in our database and you will observe our security safeguards and exercise reasonable caution when using this site. Specific institutional and technological security safeguards include:

1. Only Voyager Sopsis employees who are authorized to handle student data are able to access the Data Management System.
2. Only school district employees and representatives that the district authorizes as school officials are permitted to access the system. It has a hierarchical permissions system. This means:
 - a) A teacher will only be able to see data for his/her class.
 - b) A Principal, Coach, or other authorized School User will be able to view all data at a given school.
 - c) An authorized district-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the district.
3. Each authorized school official is given a UserID and Password valid only for the duration of the academic year, including a summer program if applicable. You must safeguard your UserID and Password, and not permit any unauthorized access to student data entered or kept in Voyager Sopsis' system.
4. Upon written request by the district, Voyager Sopsis will destroy any student data for districts who no longer participate in a Voyager Sopsis reading program. Voyager Sopsis will provide written verification that the data has been destroyed as requested.
5. If a district has not used any Voyager Sopsis product for a period of ten years, Voyager Sopsis will provide written notice that the student data pertaining to their district will be destroyed, unless the district requests the records be kept. Upon destruction, Voyager Sopsis will provide written verification that the data has been destroyed. (Voyager Sopsis will delete all data upon termination of the contract, after a year of no renewals or activity, and/or at the request of the district.)
6. Voyager Sopsis uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.

Section II.6: Disclosure Notification

We notify LEAs within 72 hours after a confirmed security breach. In this case we will collaborate closely with how the district wants to handle the communication to its parents and teachers and any law enforcement agencies that need to be informed.

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

Under the terms of our contracts with schools, we agree to act as a "School Official" as defined by FERPA, meaning that we:

1. Perform an institutional service or function for which the school or district would otherwise use its own employees
2. Have been determined to meet the criteria set forth in the school's or district's annual notification of FERPA rights for being a School Official with a legitimate educational interest in the education records
3. Are under the direct control of the school or district with regard to the use and maintenance of education records
4. Use education records only for authorized purposes and will not re-disclose from education records to other parties (unless we have specific authorization from the school or district to do so and it is otherwise permitted by FERPA)
5. The company users a 3rd party, iKeepSafe, to audit our compliance with FERPA. For proof of our programs' audited compliance, see <https://ikeepSAFE.org/products/>.

As you use our site, you will enter student data or interact with student data that has already been entered. Federal law (the Family Educational Rights and Privacy Act, "FERPA") allows a school district to release student records to an organization that is "conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests... [or] improving instruction." However, FERPA requires limitations on disclosure of those records and implementation of appropriate security measures to protect those records. To help your school district comply with FERPA, Voyager Sopsis has adopted certain practices, and requires that educators using this site fulfill certain responsibilities to safeguard student data.

Full information on our practices and your responsibilities regarding student data can be found here: <https://www.voyagersopsis.com/terms-conditions>

Section III.5: How Student Data is Protected:

We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from you. We will implement reasonable and appropriate safeguards when collecting student data from you and when storing that student data in our database and you will observe our security safeguards and exercise reasonable caution when using this site. Specific institutional and technological security safeguards include:

1. Only Voyager Sopsis employees who are authorized to handle student data are able to access the Data Management System.
2. Only school district employees and representatives that the district authorizes as school officials are permitted to access the system. It has a hierarchical permissions system. This means:
 - a) A teacher will only be able to see data for his/her class.
 - b) A Principal, Coach, or other authorized School User will be able to view all data at a given school.
 - c) An authorized district-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the district.
3. Each authorized school official is given a UserID and Password valid only for the duration of the academic year, including a summer program if applicable. You must safeguard your UserID and Password, and not permit any unauthorized access to student data entered or kept in Voyager Sopsis' system.
4. Upon written request by the district, Voyager Sopsis will destroy any student data for districts who no longer participate in a Voyager Sopsis reading program. Voyager Sopsis will provide written verification that the data has been destroyed as requested.
5. If a district has not used any Voyager Sopsis product for a period of ten years, Voyager Sopsis will provide written notice that the student data pertaining to their district will be destroyed, unless the district requests the records be kept. Upon destruction, Voyager Sopsis will provide written verification that the data has been destroyed. (Voyager Sopsis will delete all data upon termination of the contract, after a year of no renewals or activity, and/or at the request of the district.)
6. Voyager Sopsis uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.



Voyager Sopris Learning
 Attn: Order Entry Department
 17855 Dallas Pkwy, Suite 400
 Dallas, Texas 75287
 Phone: (800) 547-6747
 Fax: (888) 819-7767
 Email: CustomerService@voyagersopris.com

Quote Number 00122627
 Created Date 6/20/2022

Quote To Beverly Campbell
 Phone (916)771-1600
 Email bcampbell@rcsdk8.org

Bill To Name Roseville City School District
 Bill To 1050 Main St
 Roseville, CA 95678
 US
 Ship To Name Roseville City School District
 Ship To 1046 Main St.
 Roseville, CA 95678
 US

Sales Executive

Sarah Durlak
 214-932-9367
sarah.durlak@voyagersopris.com

| Description | Product Code | Quantity | Sales Price | Total Price |
|---|--------------|----------|-------------|-------------|
| Vmath Student Math Pack (Print and Digital), Level C | 338221 | 30.00 | \$45.00 | \$1,350.00 |
| Vmath Student Math Pack (Print and Digital), Level D | 338239 | 30.00 | \$45.00 | \$1,350.00 |
| Vmath Student Math Pack (Print and Digital), Level E | 338247 | 30.00 | \$45.00 | \$1,350.00 |
| Vmath National Teacher Materials (Print and Digital), Level C | 338378 | 4.00 | \$337.00 | \$1,348.00 |
| Vmath National Teacher Materials (Print and Digital), Level D | 338386 | 4.00 | \$337.00 | \$1,348.00 |
| Vmath National Teacher Materials (Print and Digital), Level E | 338394 | 4.00 | \$337.00 | \$1,348.00 |
| TransMath 3rd ed. Teacher Kit Level 1 Developing Number Sense Print and Digital | 347119 | 4.00 | \$404.00 | \$1,616.00 |
| TransMath 3rd ed. Level 1 Developing Number Sense Print and Digital Student Set | 346853 | 68.00 | \$55.00 | \$3,740.00 |

Total Price \$13,450.00
 S&H \$1,345.00
 Tax \$1,210.50
 Total Due \$16,005.50

Comments

*Prices included herein are exclusive of all applicable taxes, including sales tax, VAT or other duties or levies imposed by any federal, state or local authority, which are the responsibility of customer. Any taxes shown are estimates for informational purposes only. Customer will provide documentation in support of tax-exempt status upon request. Pricing is valid for 60 days unless otherwise specified on this quote. Unless otherwise provided herein, Voyager Sopris will invoice the total fees set forth above upon receipt of customer's PO/acceptance. Payment is due net 30 days of invoice.

All academic school year licenses begin August 1 and end July 31 annually and all Summer subscription licenses begin May 1 and end July 31, regardless of purchase date.

- Additional Support Services purchased separately from subscription licenses/packages (e.g., webinars or additional onsite and/or virtual training hours) must be used within 12 months from the received date of the PO acceptance of the applicable quote.
- A customer-designated account administrator contact name and email address are required for all subscriptions and service orders.



Order Term

This order quote and the associated confirming purchase order or other customer confirmation of this quote serve as an agreement for this order which becomes effective upon its acceptance by both parties. Unless otherwise agreed by Voyager Sopris and customer in writing, the licenses, products, and/or services purchased pursuant to this quote will begin on or about the start date and continue in effect for the period set forth in this quote. Unless otherwise set forth in this quote or agreed to by Voyager Sopris and customer in writing: all subscription licenses under the order shall have the same start and end dates; all subscription products and services are deemed delivered upon provisioning of license availability; and all subscription licenses and associated services must be used within the subscription or service period specified herein - unused subscription licenses or services are not eligible for refund or credit. On-site training may be fulfilled with a virtual training equivalency, as needed, of up to six instructional hours per day.

Order Process

To submit an order, please fax this quote along with the applicable Purchase Order to 888-819-7767, send by email to customerservice@voyagersopris.com, or send to your sales representative's email address listed above. NOTE: Each Purchase Order must include the correct quote order number as provided on this quote, and should attach this quote.

Order Acceptance

All Voyager Sopris subscriptions, products and/or services are offered subject to Voyager Sopris' standard license and terms of use (the "License Terms"), available at: <https://www.voyagersopris.com/terms-conditions>, as supplemented by this quote. By placing an order, customer confirms its acceptance of the License Terms and this quote, which together with any previously awarded proposal and/or any other associated agreement entered into by Voyager Sopris and customer regarding the subscriptions, products and services in this quote, constitute the entire agreement between customer and Voyager Sopris regarding such subscriptions, products, and services (the "Agreement"). Customer and Voyager Sopris agree that the terms and conditions of the Agreement supersede any additional or inconsistent terms or provision in any customer drafted purchase order, or any communications, whether written or oral, between customer and Voyager Sopris relating to the subject matter hereof, which shall be of no effect. In the event of any conflict, the terms of the Agreement shall govern.