

**AGREEMENT
REGARDING DATA SECURITY AND PRIVACY**

Agreement dated as of August 5, 2020, by and between the East Rockaway Union Free School District (“District”) and Voyager Sopris Learning, Inc. (“Contractor”).

WHEREAS, the District has entered into a contract or other written agreement, as defined in Part 121 of the Commissioner’s Regulations, with Contractor for certain services or products, a copy of which is annexed hereto; and

WHEREAS, Contractor is a third-party contractor as defined in Part 121 of the Commissioner’s Regulations, that will receive student data or teacher or principal data from the District pursuant to said contract or other written agreement for purposes of providing services to the District; and

WHEREAS, the parties agree that if any provision of this Agreement conflicts with a provision of said contract or other written agreement, the provision as set forth in this Agreement shall supersede and prevail over said other provision;

NOW, THEREFORE, in consideration of the mutual covenants, conditions and agreements contained herein, and for other good and valuable consideration, including the above-referenced contract or other written agreement, the Contractor and the District hereby agree as follows:

A. The Contractor shall comply with all District policies and state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the District’s Parents’ Bill of Rights and Supplemental Information, annexed hereto and incorporated herein as Attachment “A”.

B. The Contractor may receive personally identifiable information from student records (“Education Records”) and/or personally identifiable information from annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release pursuant to Education Law § 3012-c and 3012-d (collectively, “PII Data”). The Contractor shall, therefore, comply with the following provisions in order to maintain the security and confidentiality of personally identifiable information:

- (i) adopt technologies, safeguards and practices in alignment with the NSIT Cybersecurity Framework;
- (ii) comply with the school district’s data security and privacy policy;
- (iii) limit the Contractor’s internal access to Education Records to individuals with legitimate educational interests;
- (iv) use PII Data only for the purposes explicitly authorized by this Agreement and not for any other purpose;
- (v) not disclose any personally identifiable information from PII Data to any other party without prior written consent, unless disclosure is required by statute or

- court order and written notice is given to the District (notice is not required if it is expressly prohibited by a statute or court order);
- (vi) maintain reasonable safeguards to maintain confidentiality of personally identifiable information in PII Data;
 - (vii) use legally mandated encryption technology¹ to protect data from unauthorized disclosure while the data is in motion or in the contractor's custody; and
 - (viii) not sell, use or disclose student, teacher or principal personally identifiable information for any marketing or commercial purpose.

C. The Contractor represents and warrants that its contract or written agreement with the District includes the Contractor's data security and privacy plan that is acceptable to the District, a copy of which is attached hereto and incorporated herein as Attachment "B". The Contractor's data security and privacy plan shall, at a minimum:

- (i) outline how the Contractor will implement State and federal data security and privacy contract requirements for the life of the contract and is consistent with the school district's data security and privacy policy;
- (ii) specify administrative, operational and technical safeguards the third-party contractor will use to protect personally identifiable information;
- (iii) show that it complies with requirements of §121.3(c) of the Commissioner's Regulations;
- (iv) specify how the third-party contractor's employees and any assignees with access to student data, or teacher or principal data receive or will receive training on relevant confidentiality laws, before receiving access to such data;
- (v) specify if the third-party contractor will use subcontractors and how it will ensure personally identifiable information is protected;
- (vi) specify an action plan for handling any breach or unauthorized disclosure of personally identifiable information and promptly notify the school district of any breach or unauthorized disclosure; and
- (vii) describe whether, how and when data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated.

D. The Contractor must notify the District of any breach of security resulting in an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employee's, assignees or subcontractors. This notification must be made in the most expedient way possible and without delay. In addition, the Contractor must notify the District of the breach of security in writing. This written notification must be sent by the Contractor in the most expedient way possible and without unreasonable delay, and not later than seven (7) calendar days after discovery of the breach of security resulting in an unauthorized release of personally identifiable information from PII Data, to the designated District representative and either personally delivered or sent by nationally recognized overnight carrier to the District. In the case of an unauthorized release of personally identifiable


¹ Encryption means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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.

information from PII Data by the Contractor or the Contractor's officers, employees, assignees or subcontractors, the Contractor must reimburse the District for all the District's costs associated with the District's obligation to notify the State's chief privacy officer, parents, students, teachers and/or principals of the unauthorized release.

IN WITNESS WHEREOF, the parties hereto have set their respective hands and seals as of the date and year first above written.

DISTRICT

CONTRACTOR

BY: 

BY: 

DATE: 12/9/2020

DATE: 12/9/2020

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

The East Rockaway Union Free School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information in education records from unauthorized access or disclosure in accordance with State and federal law, and establishes the following parental bill of rights:

1. Students' personally identifiable information will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and federal Law;
2. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third-party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
3. Parents have the right to inspect and review the complete contents of their child's education record;
4. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
5. A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov.data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234;
6. Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Privacy Officer at 516-887-8300 Ext. 440 or by mail to the Data Privacy Officer, East Rockaway School District, 443 Ocean Avenue, East Rockaway, NY 11518. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov.data-privacy-security>, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 5178-474-0937.
7. Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's personally identifiable information occurs;

8. Parents can expect that educational agency workers who handle personally identifiable information will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect personally identifiable information;
9. In the event that the District engages a third party provider to provide, deliver or facilitate student educational services, the contractor or subcontractors will be obligated to adhere to the District's data security and privacy policy and with State and federal laws to safeguard students' personally identifiable information, as well as to this Bill of Rights and required supplemental information for each contract.
10. This Parents' Bill of Rights will be included with every contract or other written agreement entered into by the District with a third-party contractor if the contractor will receive student data or teacher or principal data. The Bill of Rights shall also be supplemented to include information about each contract or other written agreement that the District enters into with a third-party contractor receiving student data or teacher or principal data, including: the exclusive purpose(s) for which PII Data will be used; how the contractor will ensure confidentiality and data protection and security requirements; the duration and date of expiration of the contract and what happens to PII Data upon the expiration of the contract; if and how the accuracy of PII Data collected can be challenged; where the student data or teacher or principal 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 and data security and privacy risks mitigated; and how PII Data will be protected using encryption while in motion and at rest.
11. Parents can request information about third party contractors by contacting the Data Privacy Officer at 516-887-8300 Ext. 440 or by mail at 443 Ocean Avenue, East Rockaway, NY 11518 or can access the information on the district's website <http://eastrockawayschools.org/departments/technology>
12. This Parents' Bill of Rights and supplemental information for contracts with third-party contractors shall be posted the district website at the following link: <http://eastrockawayschools.org/departments/technology>

* * *

**PARENTS' BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT**

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor verifies the following supplemental information to the Parents' Bill of Rights regarding data privacy and security:

(1) The student data or teacher or principal data (collectively, "PII Data") received by the Contractor will be used exclusively for the following purpose(s):

Contractor and its agents, employees and subcontractors, if any, shall use PII Data solely for the purpose of providing services as set forth in the parties' contract or other written agreement. Contractor and its agents, employees and subcontractors will not use PII Data for any other purposes. Any Data received by or by Contractor or any of its agents, employees, subcontractors or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

(2) The Contractor will ensure the confidentiality of PII Data that is shared with subcontractors or other persons or entities as follows:

In the event that Contractor subcontracts with an outside entity or individual in order to fulfill its obligations to the District, Contractor ensures that it will only share PII Data with such subcontractors if those subcontractors are contractually bound to observe obligations to maintain data privacy and security consistent with those required of Contractor pursuant to the Agreement. Contractor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII Data in its custody consistent with the data protection and security requirements of district policy, and state and federal law and regulations by (*Voyager Sopris Learning, Inc. does not utilize the services of subcontractors*).

(3) The duration of Contractor's services begins on (*N/A*) and ends on (*N/A*), as set forth in the parties' contract or other written agreement. Once the contractor has completed its service to the district, records containing PII Data received by the Contractor will be disposed of as follows:

All PII Data will be disposed of in accordance with the instructions of the District, and will be: (a) delivered to the District or transitioned to a successor contractor, at the District's option and direction, (b) de-identified and/or (c) deleted from Contractor's computer systems and destroyed. Contractor will provide written confirmation of such disposition to the District, upon written request.

(4) A parent, student, teacher or principal can challenge the accuracy of PII Data received by the Contractor as follows:

In the event that a parent or eligible student wishes to challenge the accuracy of PII Data

concerning that student that is maintained by Contractor or its subcontractors, such challenge may be processed through the procedures provided by the applicable educational agency or institution for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that Contractor is notified of the outcome of any such errors made by Contractor, it will promptly correct any inaccurate data it or its subcontractors or assignees maintain. The District or the applicable New York education agency/institution will use FERPA's data correction procedures, as applicable, to update any data that is not a result of an error made by Contractor or its subcontractors.

(5) The following is how PII Data will be stored and what security protections will be taken by the Contractor:

All Data in Contractor's possession will be securely stored (*Voyager Sopris Learning's application and database servers are housed, in a dedicated, secondary redundant, remote, secure location within the continental U.S., within a Tier 3 Data Center Managed by AT&T.*). Contractor represents that the following security protections, including encryption where applicable, will be in place to ensure that PII Data is protected. (*Describe the following, as applicable*):

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls

Voyager Sopris Learning, Inc. will utilize Firewall ports, and 128-SSL Encryption to secure data throughout the life of the contracts.

THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

- (i) Contractor will implement State and federal data security and privacy contract requirements for the duration of its contract that is consistent with the school district's data security and privacy policy by:
[Voyager Sopris Learning, Inc. will utilize Firewall ports, and 128-SSL Encryption to secure data throughout the life of the contracts. Voyager Sopris Learning's application and database servers are housed, in a dedicated, secondary redundant, remote, secure location within the continental U.S., within a Tier 3 Data Center Managed by AT&T.](#)
- (ii) Contractor will use the following administrative, operational and technical safeguards to protect personally identifiable information:
[Voyager Sopris Learning, Inc. will utilize Firewall ports, and 128-SSL Encryption to secure data throughout the life of the contracts. Voyager Sopris Learning's application and database servers are housed, in a dedicated, secondary redundant, remote, secure location within the continental U.S., within a Tier 3 Data Center Managed by AT&T.](#)
- (iii) Contractor has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information attached to its contract or written agreement with the District, or as follows:
[Please see Voyager Sopris Learning, Inc.'s Data Privacy Policy attached.](#)
- (iv) Contractor's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:
[We use the KnowBe4 platform and require each of our employees and contractors to take a handful of courses each year.](#)
- (v) Contractor will use the following subcontractors and will ensure that personally identifiable information received by its subcontractors is protected, as follows:
[N/A](#)
- (vi) Contractor will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the school district of any breach or unauthorized disclosure as follows:
[Voyager Sopris Learning performs external penetration testing and has a written incident response process where the affected customers are notified within 72 hours of a detected security breach.](#)
- (vii) Data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated as follows:
[Destroyed as soon as commercially possible.](#)

Privacy Statement for Voyager Sopris Learning, Inc. Data Management System

This site provides you with access to Voyager Sopris' Data Management System. This system is an integral component of Voyager Sopris' curriculum products and provides valuable reporting, instructional recommendations, and other resources used by teachers and other instructional leaders in conjunction with Voyager Sopris' curriculum with the goal of improving student performance.

This statement describes the privacy and security practices Voyager Sopris employs for this site. We have adopted these practices to protect you, the students, and the school district, and to enable each of us to comply with applicable legal requirements. Use of this site requires district acceptance of the practices outlined in this statement.

Two types of personally identifiable information are used on this site: **your personal data** and **student data**.

Your Personal Data

Collection: Voyager Sopris collects information from you as you use this site. For example, you must enter certain personally identifiable information, including your name, e-mail address, and phone number. We use this information to verify your identity and prevent unauthorized access to your account and to contact you in connection with your use of this site.

In addition to the information you provide, Voyager Sopris collects information about your use of this site through tracking, cookies, and log files, as described in our general [Terms of Use](#) statement.

Protection: Because you enter your personal data, you control its accuracy. If you discover that your personal data is inaccurate or if it changes, you may make corrections by notifying us at support@voyagersopris.com or 888-399-1995. We will not share your personal data collected through this site with third persons without your consent. However, your personal data will be available to authorized users from your school district who have permission from the school district to access it. We will not use your personal data collected through this site for any purpose other than providing you with access to this site and the associated services. We will use the same security to protect your personal data that we use to protect student data collected through this site.

Student Data

As you use this 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 Sopris has adopted certain practices, and requires that educators using this site fulfill certain responsibilities to safeguard student data. The following statement explains our practices and your responsibilities regarding the student data you enter on this site.

Additionally, Voyager Sopris operates in compliance with the Children's Online Privacy Protection Act ("COPPA"). Voyager Sopris will not knowingly collect or use personally identifiable information from anyone under 13 years of age.

Student Data Security and Confidentiality Statement

Purposes of Data Entry: You control what student data is entered on this site. Student data entered on this site should be limited to information that is relevant to the legitimate educational purpose of improving student performance. We will not ask you to enter, and you are instructed not to enter, data about students that is not relevant to this legitimate educational purpose.

Therefore, only a minimum amount of personally identifiable student data required for the setup of the system is requested. We require student first name, student last name, and student identification number. Additional data, not specific to the student, is also required to complete system setup, including the teacher first and last name, class name, grade level, and school name. Student demographic data, for the purposes of optional disaggregated reporting, is requested separately from the initial setup data and is obtained only with written permission from your district.

Use, Disclosure, and Storage: We will use the student data to provide the services to your school district. We will not keep the student data after you or the school district instructs us to delete it. You may not disclose or otherwise use the student data entered on this site for any unauthorized purposes.

We will only disclose student data to authorized employees or representatives of the school district, and will not knowingly disclose the student data to any third person without express written authorization. When, at the request of the district, we acquire assessment or other information, including personally identifiable student data, from a third party source we treat that information with the same confidentiality and security safeguards as though it were provided directly by the district. Additional agreements may be required by the third party to authorize transmission of data to Voyager Sopris.

Your district may from time to time request that Voyager Sopris provide student data to third parties of its choosing. We will do so with written authorization, which acknowledges that Voyager Sopris is providing that data as your district's agent and that once the data is received by the third party, Voyager Sopris no longer has any control over the use or disposition of the data.

We may also use aggregated data in our research, product development, and marketing. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, we do not use personally identifiable student data to market any products or services directly to students or their parents.

In the event that Voyager Sopris wishes, from time to time, to release aggregated data that identifies your school or school district by name, Voyager Sopris will enter into a separate agreement with you to authorize release and publication.

Data Quality: You are responsible for keeping the student data that you enter accurate, complete and up-to-date. If you recognize that student data is inaccurate, incomplete, or out-of-date, you are 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.

Security Safeguards: 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 Sopris 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 Sopris' system.
4. Upon written request by the district, Voyager Sopris will destroy any student data for districts who no longer participate in a Voyager Sopris reading program. Voyager Sopris will provide written verification that the data has been destroyed as requested.
5. If a district has not used any Voyager Sopris product for a period of ten years, Voyager Sopris 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 Sopris will provide written verification that the data has been destroyed.
6. Voyager Sopris uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.

When you use this site, you consent to our privacy practices and agree to accept the responsibilities outlined in this statement.

Terms of Use

User Responsibility

By using this web site, you are agreeing to be bound by these Terms and Conditions of Use, all applicable laws and regulations, and agree that you are responsible for compliance with any applicable local laws. If you do not agree with any of these terms, you are prohibited from using or accessing this site. All Users are responsible at all times for their use of the Voyager Sopris Learning Web Site. Voyager Sopris assumes no liability regarding any use of the Web Site by any person. At any time, and in its sole discretion, Voyager Sopris may terminate, limit, or modify access of any person to the Web Site.

Educational Use Only

Each User agrees to access the Web Site and to use the Services provided by Voyager Sopris only for educational purposes, and for no commercial purposes whatsoever.

No Interruption

Users shall not attempt to disrupt or interrupt the operation of the Web Site. Users shall not use the Web Site in any manner that could damage, impair, or interfere with any person's use of, the Web Site.

Connection Charges

Users are responsible for all charges associated with connecting to the Web Site.

Public Communications and Email

Voyager Sopris may provide certain Users the facility for posting communications in the form of e-mail, web pages, or other similar communication. Such postings are intended for public consumption and the author shall have no expectation of privacy in such communications. Such communications may not contain offensive material as defined herein. Users may post only their original work. Voyager Sopris will not be responsible for the content of materials posted by Users, and does not attempt to review all communications made to or through the Web Site. Voyager Sopris retains the right, but has no obligation, to monitor such postings, either randomly or in response to inquiries, or both, in order to detect and remove any material that Voyager Sopris, in its sole discretion, believes to be offensive, obscene, slanderous, or in any way contrary to law or to Voyager Sopris policies. In posting any communications, the User grants to Voyager Sopris a fully-paid, perpetual, worldwide, and royalty-free right to copy, display, and distribute and such communications in such form and manner as Voyager Sopris in its sole discretion may deem beneficial to its subscribers.

“Offensive Material” includes, but is not limited to, material that:

- Is obscene, offensive, indecent, pornographic, sexually explicit or abusive;
- Contains any racial, religious, or ethnic insult;
- Contains false or misleading statements of fact;
- Constitutes impersonation of another person;
- Is slanderous, libelous or defames any person or entity;
- Causes injury to any person or entity;
- Infringes the privacy or intellectual property rights of any person or entity;
- Is contrary to law or to public policy;
- In any way violates this Agreement or any Voyager Sopris policy;
- Includes any survey, contest, pyramid scheme, or chain letter;
- Advertises or offers to sell or buy any goods or services for any commercial purpose;
- Collects or harvests information about others without their express consent;
- Solicits funds, except for the benefit of Customer and for a charitable or educational purpose;
- Or contains any software virus or other code or routine designed to interrupt, destroy, or limit the functionality of any computer.

Links

Voyager Sopris may on its Web Site provide hyperlinks and pointers to other sites on the Internet maintained by third parties. Such links do not constitute an endorsement by Voyager Sopris. Voyager

Sopris and its affiliates are not responsible for the content, availability, accuracy, or currency of other sites. No person may link to www.voyagersopris.com without the express permission of Voyager Sopris.

Copyrights

Voyager Sopris and its Licensors are the owners of all content and materials on the Web Site, which is protected by copyright and other laws. Users may, on an occasional and irregular basis, disseminate an insubstantial portion of the content from the Web Site, for any non-commercial purpose, without charge, and may transmit the same, in tangible non-electronic form only, to a limited number of individuals. In transmitting any such material, Users must include all copyright and other proprietary right information unchanged in form, must include original source attribution, and must include the phrase "Used with the Permission of Voyager Sopris, Inc." Users may not post any content of the Voyager Sopris Web Site to any newsgroup, mail list or electronic bulletin board. Users may not reproduce, transmit, sell, distribute, or in any way exploit the Web Site or any portion thereof for any commercial use.

Limitation of Liability / No Warranty

Voyager Sopris Learning, its employees, and its authors make no representations, and assume no liability, legal or otherwise, for the accuracy, reliability, applicability, use, or misuse of the information and strategies described on this website or in its publications. All functionalities are provided "as is", and without warranties of any kind, express or implied. To the fullest extent permitted by law, Voyager Sopris expressly disclaims any warranty of merchantability and fitness for a particular purpose, and moreover disclaims any warranty of title, compatibility, security, accuracy, and non-infringement. The content provided may include facts, views, opinions and recommendations of persons other than Voyager Sopris, which are deemed by Voyager Sopris to be of interest to Users. Neither Voyager Sopris nor its Licensors guarantee or warrant the accuracy, completeness, or timeliness of such content, or otherwise endorse the authors. Voyager Sopris intends no portion of the content as professional advice, particularly with regard to determining and implementing the best course of action for an individual student.

General

This Policy sets forth the entire understanding and agreement between the parties with respect to the subject matter hereof.

Modification

We reserve the right to modify this Policy at any time by posting an amended Policy that is always accessible on this site's home page and by giving you prior notice of such amendments. Your continued use of this Website after a modification indicates your acceptance of the amended Policy.

Governing Law & Venue

Any claim relating to the Voyager Sopris web site shall be governed by the laws of the State of Texas without regard to its conflict of law provisions. Any dispute will be subject to the exclusive jurisdiction of the courts located within Dallas County in the State of Texas, and User hereby submits to the personal jurisdiction of such courts.

Indemnity

Users agree to indemnify and hold Voyager Sopris and (as applicable) Voyager Sopris's parent, subsidiaries, owners, affiliates, officers, directors, consultants, suppliers, agents and employees harmless from any claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your breach of the Terms and Conditions, or your violation of any law or the rights of a third party.

Severability

If any part of these Terms of Use / Privacy Policy is held to be unenforceable, such holding shall not affect the validity of the other provisions of the Terms of Use, which shall remain in full force and effect.

Survival

The following Sections survive any termination or expiration of this Agreement: No Warranty, Severability, Indemnity, Governing Law.

Still have questions?

If you have any questions about this terms of use and privacy statement, please contact: customerservice@cambiumlearning.com.

Note: Any updated policies will be posted to the service immediately.