EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and "Contractor" is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Valley Stream UFSD 30 (the "District") and Heinemann, a division of Greenwood Publishing Group LLC (“Contractor”) to the contrary, Contractor agrees as follows:

1. Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Contractor shall not disclose Protected Data other than to those of its employees or subcontractors or third party service providers who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place reasonably designed internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ('CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information actually provided by the District to Contractor through use of Math Expressions (“service”) rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in 99.3 ofFERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is

confidential and not subject to release under the provisions of Education Law "3012-c and 3012-d.

2. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law 2-d as applicable to the service it provides. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy, which are attached to this Rider, Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data caused solely by Contractor, its subcontractors, and/or assignees's negligence or omission. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, upon sixty (60) days' written request by the District prior to such expirations, non-renewal or termination, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify how officers or employees of the Contactor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;

b. Comply with the data security and privacy policy of the District which is attached to this Rider; Education Law 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or subcontractors, including third party service providers, that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract. The Contractor may use de-identified information for evaluation, research and development of educational products and services;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    i. except for authorized representatives of Contractor such as a subcontractor or assignee, like a third party service providers, to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
h. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further,
Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be

b. How the Contractor will ensure that the subcontractors, persons or entities that the C ontractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
e. 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, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Contractor shall promptly notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of confirmation of the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District at the following address:

Superintendent of Schools
valley Stream UFSD 30
175 N. Central Avenue, Suite 220
valley Stream, NY 11580

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure may be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) 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 899-aa(6)(a).

8. Except as provided in Education Law 2-d(6)(d), in the event Contractor violates Education Law 2-d, said violation may be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data may be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data may be punishable by a civil penalty of up to ten thousand dollars ($ 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 899-aa(6)(a).

9. Contractor agrees that it will reasonably cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any actual costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is solely attributable to the Contractor or its subcontractors's negligence or omission.

10. Upon termination of this Agreement, with sixty (60) days written notice, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing industry standard methods of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using industry standard methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event a Contractor engages a subcontractor to perform its contractual obligations, equivalent data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the
Plan.

Contractor: Heinemann, a division of Greenwood Publishing Group LLC

Signature: Ashley Poreda Date: 12/18/2025

Printed Name:
Ashley Poreda Title: Lead Contracts Specialist

EXHIBIT "A"

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State Education Law 52-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law 52-d. This document contains a plain-English summary of such rights.

- A student's personally identifiable information cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Valley Stream Union Free School District Thirty.
- State and Federal Laws protect the confidentiality of personally identifiable student information, and 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.
- A complete list of all student data elements collected by New York State is available for review at the following website: http://www.p12.nvsed.gov/irs/sirs

The list may also be made available by writing to:

Office of Information & Reporting Services
New York State Education Department
Room 863 EBA,
89 Washington Avenue
Albany, NY 12234

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

valley Stream UFSD 30
Attn: Data Protection Officer
175 N. Cerfral Avenue, Suite 220
Valley Stream, New York 11580
Marcela Moran
516434-3642

OR

Chief Privacy Officer
New York State Education Department

89 Washington Avenue Albany,
NY 12234
Email: CPO@mail.nysed.gov

- Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

    - The exclusive purposes for which the student data or teacher or principal data will be used.
- How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
    - When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.
    - If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
    - Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

- Third-party contractors are also required to:

    - Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data; o Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
    - Not use educational records for any other purpose than those explicitly authorized in the contract;
    - Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
    - Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
    - Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law 52-d;
    - Notify the District of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

- Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
- Provide a signed copy of this Bill of Rights to the District thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

- This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Contractor:

Heinemann, a division of Greenwood Publishing Group LLC

Date: 12/18/2025

Signature: Ashley Poreda

Title: Lead Contracts Specialist

Printed Name: Ashley Poreda

EXMBIT "B"

Contractor's | Supplemental Information

Name of Contractor	Heinemann, a division of Greenwood Publishing Group LLC
Description of the purpose(s) for which Contractor Wilf receive/access Pil	HNM will only use data in connection with District's use of HNM's products.
Type of PI' that Contractor will receive/access	Check all that apply: X Student Pll O APPR Data
Agreement Term	Agreement Start Date:11/21/2025 Agreement End Date: 11/20/2026
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Contractor by State and federal laws and regulations, and the Agreement. (check applicable option): O Contractor will not utilize subcontractors. X Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, with sixty (60) days written notice, Contractor shall: Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PI' will do so by contacting the District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected (check all that apply): X using a cloud or infrastructure owned and hosted by a third-party. O Using Contractor owned and hosted solution. O Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: HNM stores all data in an AWS Hosting facility in the United States. HNM has implemented and maintains reasonable organizational, technical, and

	administrative controls and is responsible for the development, operation, maintenance, and use of our cloud-hosted applications and data required for customers to participate in our learning platforms. Physical security controls are managed by our hosting partner, Amazon Web Services (AWS). Our data management procedures include the following: all user data are encrypted using standard Internet protocols; all user data on our interface are transferred over HTTPS; all user data in transit are protected by TLS 1.2; all user data are housed on a scalable hosting architecture; all user data are stored behind AES-256 encryption algorithms. For additional information, please refer to HNM's Privacy Policy at https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy . Additionally, access to data is based on a least-privileged model, where individuals are only granted the rights necessary to complete their job functions.
Encryption	Data will be encrypted while in motion and at rest.

Contractor: Heinemann, a division of Greenwood Publishing Group LLC

Signature: Ashley Poreda Date: 12/18/2025

Printed Name: Ashley Poreda Title: Lead Contracts Specialist

EXHIBIT "C"

Contractor's Data Security & Privacy Plan

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy

Skip to main content

Privacy Policy for Heinemann Products

Last Updated: October 30, 2020 (prior version effective September 1, 2014)

Heinemann, a division of Greenwood Publishing Group, LLC (“**Heinemann,**” “**we**” or “**us**”) is a publisher of professional resources and provider of educational and professional development services for teachers and students, from grade Pre-K through college. We provide educational and professional development materials and related services for teachers and students via a set of online learning platforms, educational software and digital applications (our "**Products**”). This Privacy Policy (this “**Policy**”) governs our privacy practices for each Product that links to this Policy. Where capitalized terms are used in this Policy without definition, their definitions may be found in Section 20.

1. Our Customers, Users and our Commitment to Privacy

We have created our Products to assist our teachers, administrators, and school/school district customers (each, a "**Customer**") in providing personalized and rewarding online educational experiences to their students. We offer a comprehensive online assessment, data management platform for Customers relative to student interviews around math, small group intensive literacy intervention support programs, and more. We believe that transparent and strong privacy practices foster these experiences, and we provide this Policy in that spirit. Our Customer agrees to this Policy and any updates, on behalf of its administrators, teachers, students, and students' parents or guardians (collectively, "**Users**"). Our Customer is responsible for collecting appropriate User consents that may be required in order to share their Users' Personal Information with us.

2. Updates to this Privacy Policy

The date on which this Policy was last revised is identified at the top of this page. We will post any updates we make to this Policy from time to time on this page. If we make material changes to how we treat our Users' Personal Information, we will notify our Customer by email and/or through a notice on the Product's home page. Any changes will become effective when we post the revised Policy or, in the case of any material changes, provide the revised Policy to our Customer. The Customer is responsible for ensuring we have an up-to-date active and deliverable email address on file, and for periodically visiting the Product's home page and this Policy to check for any updates.

3. Our Compliance With COPPA And FERPA

We recognize the sensitive nature of Personal Information concerning students under age 13, and concerning PreK-12 students generally, where the information is contained in a school's educational records. This Personal Information is protected under either or both of the following federal statutes: COPPA and FERPA. Our privacy practices comply with both COPPA and FERPA.

4. The Scope of Our Privacy Policy

This Policy governs our privacy practices with respect to all Personal Information that Users submit, or that we collect in connection with our Products. This Policy governs not only our practices with respect to students' Personal Information, but also with respect to the Personal Information of teachers and school administrators who use our Products.

5. Consent from Schools regarding Students' Personal Information

COPPA permits a school, acting in the role of "parent," to provide required consents regarding Personal Information of students who are under the age of 13. Where a school is the subscriber to

our Products, we rely on this form of COPPA consent. We provide the school with this Policy, to ensure that the school, in providing its COPPA consent, has full information and assurance that our practices comply with COPPA.

FERPA permits a school to provide educational records (including those that contain students' Personal Information) to certain service providers without requiring the school to obtain specific parental consent. FERPA permits this where the service provider acts as a type of “school official” by performing services, for example, that would otherwise be performed by the school's own employees. We fulfill FERPA requirements for qualifying as a school official by, among other steps, giving the school direct control with respect to the use and maintenance of the education records at issue (including associated personal information), and refraining from re-disclosing or using this Personal Information except for purposes of providing our Products to the school. We comply with FERPA by relying on this form of consent.

6. Access and Control of Personal Information

School administrators and (where applicable) teachers hold access to Personal Information of the students for whom they are responsible, and they are able to update this information in the manner permitted by our Products. School administrators and teachers are similarly able to access and update their own Personal Information. Users should contact their schools if they have questions about their data, including third parties with whom their data may be shared, and how to receive a copy of their data. The parents of a student can obtain access — through their child's school — to information concerning their child that is available on our Products. To do so, the parent should follow the school's procedures for access under FERPA. We cooperate with and facilitate the school's response to these access requests. We limit access to Personal Information to only our employees and Our Service Providers (i) who have a need to know such information, and (ii) who use the information only for the educational purposes of operating, maintaining and supporting our Products and delivering our services.

7. Consents from Other Users Who are Not Students

In addition to our Customers’ obtaining consents regarding Personal Information of Users other than students (such as teachers and school administrators) on our behalf, we may also obtain consents regarding such Personal Information. To obtain these consents we (a) notify the Users of our privacy practices by including links to this Policy within our Products, and (b) rely on their continued use of our Products to indicate their consent to this Policy.

8. The Types of Information We Collect

We limit our collection of Personal Information to no more than is reasonably necessary for the User at issue to experience our Products. Specifically, we collect the following types of information:

1. **School Administrator Information:** we collect registration information from a school administrator when the school administrator activates the school's subscription account, which may include the school administrator's own first and last name, business address and phone number, date of birth, email address, profile information and username;
2. **Teacher Information:** we collect registration information from a teacher or school administrator when the teacher (or school administrator) activates the teacher's account, which may include the teacher's first and last name, business address and phone number, date of birth, email address, profile information and username; additionally, we may collect information that constitutes Performance Review Data;
3. **Student Information:** we collect registration information from a teacher or school administrator when the teacher (or school administrator) activates the account of an individual student, which may include the student's first and last name, student ID numbers, email address, username and other information which may include gender, race, ethnicity and other demographic information, learning level and performance data. We may combine information about a student with information about his or her school, such as its location;
4. **Student Parent/Guardian Information:** we collect information about a student's parent or guardian, such as names and email addresses, and we may associate it with the student's information;
5. **Schoolwork Information:** we collect information contained in student homework, assignments, student compositions and reports, tests, test results, grades, and other exchanges over our Products;
6. **School Administrator or Teacher submitted information:** we collect information and content submitted by a school administrator or teacher, such as lesson plans and notes;
7. **User-Generated Content:** we collect information that students and other Users provide in connection with submitting user-generated content, and participating in collaborative features of our Products (where applicable). Examples of user-generated content that might contain Personal Information include notes, stories, responses to surveys, questions and teacher assignments (either in text, image, audio, or video format), responses to student's submissions (either in text, image, audio, or video format), drawings that allow text or free-hand entry of information, activities, game play, assessments, and other information provided in open-text and open-form fields or posted to a bulletin board viewable by others. If a teacher chooses not to set individual passwords for his or her students' accounts, then other students may be able to access an individual student's notes or other work;
8. **Usage Information:** we collect usage, viewing, analytics, and technical data, including search queries, device identifiers and IP addresses, relating to Users of our Products;
    1. **For certain of our Products, the name and email address of an individual to whom a User wishes to send content from the Products.** We use the information only to send the message, and we do not retain it.
    2. **Information about how, where, in a general sense (based on IP address), when, and for how long a User accesses and uses our Products, as well as what content they view, what actions they take (including, for example, clicks, touches, and hovers using a mouse), and how they navigate through our**

Products. We may use cookies, pixel tags, and other technologies to collect this information, as further explained in Section 10.

3. **Information from and about the User's device, such as mobile device type, browser type and version, operating system name and version, IP address, and referring URL.** We collect this information automatically when a User accesses our services, to help us understand usage, diagnose problems, administer our Products, and provide support.
4. **Correspondence.** Records and copies of your correspondence (including email addresses) if you contact us.
5. **Financial Information.** Details of transactions you carry out when using our Products and of the fulfillment of your orders. You may be required to provide financial Information before placing an order for our Products.
6. If we discover that we have collected information in a manner inconsistent with the requirements of COPPA or FERPA, we will either (a) delete the information or (b) promptly seek requisite consents before taking further action concerning the information.

9. How We Collect Personal Information

Our Products collect Personal Information in several ways. School administrators and teachers provide Personal Information during the registration process. Teachers and students also submit Personal Information during the normal operation and support of our Products. They submit this information, for example, when creating and responding to teaching assignments and student submissions, and otherwise engaging in educational and other activities available on our Products. Heinemann also collects usage information through technology, such as cookies, as further explained in Section 10 below.

10. Cookies

Heinemann collects usage information through technology, such as cookies, pixel tags, flash cookies, browser analysis tools, server logs, web beacons, and persistent identifiers. We use cookies, IP addresses, and other persistent identifiers to authenticate users in order to ensure that only authorized individuals are permitted access to our Products, and so that we can understand how a User engages with our Products, such as identifying what links are clicked and what content is accessed and for how long. This information allows us to improve our user interface and create a better product, such as by making commonly accessed content easier to reach or by more prominently displaying content that has been less frequently accessed.

Certain features (or all features) of our Products may be hosted on third party sites, and in those instances the collection activities described above may be undertaken by this third party, under our direction and control and consistent with this Policy. Most information we collect using technological means is collected only in a non-identifiable way where no information that could be

linked to an individual User is used, such as for website optimization and tracking website traffic patterns. If Personal Information is collected, this Policy governs how we use Personal Information.

11. How We Use Personal Information

In addition to the uses described above, and subject to any restrictions imposed by applicable laws or our agreement with our Customer, we may use and disclose the Personal Information we collect for the following purposes:

1. To provide our Customer and their authorized Users with the content and features available through our Products and to tailor and optimize the use of any of our Products to the needs of a particular school, classroom or student;
2. To permit school administrators and teachers to review students' work, monitor students' performance and progress, plan lesson, and otherwise support instruction;
3. To permit parents and guardians to review their children's work and monitor their performance and progress;
4. To offer students immediate feedback and continuous support, permit them to access information shared by their teachers, suggest other content or activities for them, help them track their own progress and maintain a file of their work, allow them to create a collection of books or other content, permit them to play games with other students, and adjust instruction to meet their needs;
5. To offer teachers and administrators immediate feedback, Product optimization recommendations, and continuous support, permit them to access information shared by other teachers or administrators such as video playback of classroom recordings for purposes of professional development, and suggest other content or activities for their lesson plans or professional development;
6. To communicate with school administrators and teachers about the applicable subscription account or transactions with us, and to send information about our Product's, content, features and usage;
7. To permit school administrators and teachers to use our Products' profile, social networking, and professional development features. These features permit the sharing of the User's username and other profile information with other Users. They also allow Users to communicate and share content with one another and, in some cases, with the public. We urge the school administrator and teacher users of our social networking features to be careful when deciding to disclose information through them;
8. To provide our Customer, as well as their administrators and teachers with various types of reports, such as reports detailing the performance and progress of a particular school district, school, classroom, or student;
9. To communicate with school administrators and teachers, subject to any communications preferences they express;
10. To ensure that our Products run properly and are presented optimally, and for Product improvement;
11. To diagnose problems, troubleshoot issues, and provide maintenance and support;

12. To personalize a Product's content and experiences for students, teachers, and other Users of the platform, such as by using the appropriate language, displaying their name on the user dashboard or permitting a student to view a profile picture of his or her teacher; and
13. To detect, investigate and prevent activities that may violate our policies or be illegal.

12. How We Use De-Identified Information

1. We do not as a rule allow third-party operators to collect Personal Information through persistent identifiers on our Products for any purpose other than the internal operations, support and maintenance of our Products. Further, we do not use, or permit third parties to use, Personal Information collected through our Products for the purpose of targeted advertising.
2. We may use aggregate information that does not permit the identification of any individual User or Customer for analytics purposes, to understand how our Products are accessed and used, and how they perform, so that we may improve upon their design and functionality and otherwise develop and improve upon our products and services, and to develop analytics studies. We may disclose these studies to third parties, including to demonstrate product efficacy;
3. Finally, we de-identify usage information in accordance with COPPA and FERPA, and use this de-identified Information, in order to develop, evaluate, and provide improved educational products and services, as permitted under COPPA and FERPA. To the extent we collect information that constitutes Performance Review Data, we protect such information as Personal Information in accordance with this Policy.

13. We Do Not Share Personal Information Except In Specific, Limited Circumstances

We use Personal Information for our internal purposes only, with the following limited exceptions. We disclose Personal Information:

- In response to the request of a law enforcement agency, governmental authority or other authorized public agency, including a request by a children's services agency or by the school at issue;
- To protect the security or integrity of our Products and associated applications and technology, as well as the technology of Our Service Providers;
- To the extent we believe necessary or appropriate to protect our rights, safety, or property and/or that of our affiliates, our customers, our users or others;
- To enable us to take precautions against liability, enforce legal rights, and to detect, investigate and prevent activities that violate our policies or that are illegal;
- If we are directed to do so by a subscribing school in connection with an investigation related to public safety, the safety of a student, or the violation of a school policy;

- If we are directed to do so by a subscribing school in connection with a student or parent/guardian request, as appropriate;
- To Our Service Providers, to permit them to provide the contracted services to us;
- In the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings), in which case the transferred information will remain subject to the terms of this Policy; and
- In other cases, if we believe in good faith that disclosure is required by law.

14. Third Party Services

We require Our Service Providers to agree in writing to terms that are no less restrictive regarding Personal Information that we share with them than the terms contained in this Policy. Upon written request, we will provide a list of Our Service Providers to our Customer. This Policy does not address, and we are not responsible for, the privacy, information, or other practices of any other third parties, including any third party operating any site or service to which our Products may link. The inclusion of a link in any of our Products does not imply our endorsement of the linked site or service. We are not responsible for the privacy, information or other practices of other organizations, such as Apple, Google, Microsoft, RIM, or any other device manufacturer, app developer, or provider of an app, social media platform, operating system, or wireless service.

15. How We Protect Personal Information.

We have implemented and maintain reasonable organizational, technical, administrative and physical security controls that are designed to protect the security, confidentiality and integrity of personal information collected through our Products from unauthorized access, disclosure, use, loss or modification. Our information security controls comply with reasonable and accepted industry practice, as well as requirements under COPPA and FERPA. We diligently follow these information security controls and periodically review and test our information security controls to keep them current.

1. **Information Security Procedures. We will:**
    - Standard of Care. Keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, modification, or disclosure;
    - Use for School Purposes Only. Collect, use, and disclose Personal Information solely and exclusively for the purposes for which Users provided to us the Personal Information, or access to it, and not use, sell, rent, transfer, distribute, modify, data mine, or otherwise disclose or make available Personal Information for our own purposes or for the benefit of anyone other than the Customer, without the Customer's prior written consent or as permitted by this Policy;

- Non-Disclosure. Not, directly or indirectly, disclose Personal Information to any person other than our employees and Our Service Providers who have a need to know, without express written consent from the Customer;
- Employee Training. Provide appropriate privacy and information security training to our employees.
- Transport Security. Use Transport Layer Security (TLS) for our transmission of all user data to and from our Products; and
- Secure Storage. Use industry standard file encryption for user data that is subject to protection under either COPPA, FERPA, or both. Where file encryption is not reasonably feasible, we employ other industry standard safeguards, protections, and countermeasures to protect such data, including authentication and access controls within media, applications, operating systems and equipment.

2. **Data Location and Security.** We use third party cloud service providers in the delivery and operation of our Product(s), and data (including Personal Information) is stored on the servers of our cloud service providers. Our contracts with our cloud service providers require them to implement reasonable and appropriate measures designed to secure content against accidental or unlawful loss, access, or disclosure. Our cloud service providers have at least the following security measures in place for their networks and systems: (i) secure HTTP access (HTTPS) points for customer access, (ii) built-in firewalls, (iii) tested incident response program, (iv) resilient infrastructure and computing environments, (v) ITIL based patch management system, (vi) high physical security based on SSAE-16 standards, and (vii) documented change control processes. To the extent we store personal information internally on our servers, we comply with the information security controls set out in Section 15.1.
3. **Data Breach Response.** In the event of a security breach involving Personal Information, we will take prompt steps to mitigate the breach, evaluate and respond to the intrusion, and cooperate and assist our Customer in their efforts with respect to (i) responding to the breach, including the provision of notices to data subjects; and (ii) engaging mutually agreeable auditors or examiners in connection with the security breach, subject to reasonable notice, access and confidentiality limitations.

16. Our Retention and Deletion of Personal Information

We retain Personal Information of Users of our Products (i) for so long as reasonably necessary (ii) to permit the User to participate with the Products, (iii) to ensure the security of our Users and our services, or (iv) as required by law or contractual commitment. After this period has expired, upon written instruction by the Customer, we will delete the Personal Information from our systems. Please understand that these deletion periods apply only to Personal Information and do not apply to De-identified Information. We retain De-Identified information in accordance with our standard practices for similar information, and do not retain or delete such information in accordance with this Policy. In addition, if requested by a Customer, we will delete from our Products the Personal Information of the Customer's Users as the Customer directs. Deleting this information will prevent

the User from engaging in some or all features of our Products. Where required by applicable law, we will delete such information and provide a certification of such deletion.

17. NY Parents' Bill of Rights for Data Privacy and Security

The New York Parents' Bill of Rights for Data Privacy and Security (the "**NY Privacy Bill of Rights**") addresses the relationship between schools and their third party contractors in addition to the schools' relationships with parents. The only elements of the NY Privacy Bill of Rights that are incorporated herein are those provisions directed to third party contractors ("**Contractor Privacy Provisions**"). Heinemann agrees to comply with the Contractor Privacy Provisions for Customers in the State of New York. In the event of a direct conflict between this Policy and the NY Privacy Bill of Rights, the NY Privacy Bill of Rights will control. The full text of the NY Privacy Bill of Rights is available at http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf.

18. Contact Us

You may contact us with questions or concerns regarding this Policy at the following address: custserv@heinemann.com

19. Do Not Track

Our Products do not change their behavior when receiving the "Do Not Track" signal from browser software.

20. Definitions

"COPPA" means the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506, including the rules and regulations promulgated thereunder, in each case as amended.
"De-identified information" means information that meets each of the following criteria: the information (i) does not identify a particular natural person; (ii) does not identify, by network Internet Protocol address, raw hardware serial number, or raw MAC address, a particular device or computer associated with or used by a person; (iii) does not identify the school at issue by name or address; and (iv) is not reasonably linkable to a particular natural person or school because of technical, legal, or other controls.
"FERPA" means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, including the Protection of Pupil Rights Amendment, including the rules and regulations promulgated thereunder, in each case as amended.
"Our Service Provider" means a third party that provides content and/or functionality for our Products, or services such as website hosting and customer service, and that has executed a written agreement containing terms regarding Personal Information that we share with them that

are no less restrictive than the terms contained in this Policy.

"Parent" means a parent or legal guardian of a student.

"Performance Review Data" means professional performance review data of teachers at Customers in the State of New York related to the teacher's effectiveness in the classroom and other measurements based upon factors including, but not limited to, student achievement or growth on state assessments or examinations, classroom observations by peers, classroom observations by trained evaluators, evaluation of lesson plans and other indicia of teacher practices. Performance Review Data includes annual professional performance data, as defined under New York state law.

"Personal Information" means information that identifies a natural person, as specified in FERPA, COPPA, the California Student Online Personal Information Protection Act, Ch. 22.2, §§ 22584 et seq. of the California Business and Professions Code, and Section 49073.1 of the California Education Code.