

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

This Virginia School Data Privacy Agreement (“DPA”) is entered into by and between the
Wythe County Public Schools (hereinafter referred to as “Division”) and
Lalio/Renaissance Learning, INC. (hereinafter referred to as “Provider”) on
March 29, 2022. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Division with certain digital educational services (“Services”) as described in Article I and Exhibit “A.”

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the Division may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 *et. seq.*

WHEREAS, the documents and data transferred from Virginia Divisions and created by the Provider’s Services are also subject to several Virginia student privacy laws, including Code of Virginia § 22.1-289.01. *School service providers; school-affiliated entities; student personal information*; and § 22.1-287.02. *Students' personally identifiable information*;

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the “General Offer of Privacy Terms” (Exhibit “E”), agree to allow other Local Educational Agencies (LEAs) in Virginia the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Division Data (as defined in Exhibit “C”) transmitted to Provider from the Division pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Code of Virginia § 22.1-289.01. *School service providers; school-affiliated entities; student personal information*; and § 22.1-287.02. *Students' personally identifiable information*. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) are transmitted to Provider from Division, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the Division. Providers shall be under the direct control and supervision of the Division.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit “A” hereto:

Renaissance software solutions. Please refer to Exhibit A for complete listing.

3. **Division Data to Be Provided**. In order to perform the Services described in this Article and Exhibit “A”, Provider shall list the categories of data collected, managed or shared as described below or as indicated in the Schedule of Data, attached hereto as Exhibit “B”:

Please refer to the attached Data Elements Collected by Product.

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used this DPA shall prevail over terms used in all the other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Division Data Property of Division**. All Division Data, user generated content or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the Division, or to the party who provided such data (such as the student, in the case of user generated content.). The Provider further acknowledges and agrees that all copies of such Division Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Division Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Division Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the Division. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the Divisions as it pertains to the use of Division Data notwithstanding the above. The Provider will cooperate and provide Division Data within ten (10) days at the Division’s request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. Provider shall cooperate and respond within ten (10) days to the Division’s request for personally identifiable information in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Division Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Division, who will follow the necessary and proper procedures regarding the requested information.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

3. **Separate Account**. Provider shall, at the request of the Division, transfer Student Generated Content to a separate student account when required by the Code of Virginia § 22.1-289.01. School service providers; school-affiliated entities.
4. **Third Party Request**. Provider shall notify the Division in advance of a compelled disclosure to a Third Party, unless legally prohibited.
5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Division Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF DIVISION

1. **Privacy Compliance**. Division shall provide data for the purposes of the DPA and any related contract in compliance with the FERPA, PPRA, IDEA, Code of Virginia § 22.1-289.01. School service providers; school-affiliated entities; student personal information; and § 22.1-287.02. Students' personally identifiable information, and all other applicable Virginia statutes.
2. **Parent Notification of Rights**. Division shall ensure that its annual notice under FERPA defines vendors, such as the Provider, as “School Officials” and what constitutes a legitimate educational interest. The Division will provide parents with a notice of the websites and online services under this agreement for which it has consented to student data collection to on behalf of the parent, as permitted under COPPA.
3. **Unauthorized Access Notification**. Division shall notify Provider promptly of any known or suspected unauthorized access. Division will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all Virginia and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Code of Virginia § 22.1-289.01. and § 22.1-287.02.
2. **Authorized Use**. Division Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Division Data or any portion thereof, including without limitation, any Division Data, metadata, user content or other non-public information and/or personally identifiable information contained in the Division Data, without the express written consent of the Division, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.
3. **Employee Obligations**. Provider shall require all employees and agents who have access to Division data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **Use of De-identified Information**. De-identified information, as defined in Exhibit “C”,

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider and Division agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, *i.e.*, twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Division Data and not to transfer de-identified Division Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the Division who has provided prior written consent for such transfer.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsections below, Provider shall dispose or delete all Division data obtained under this agreement when it is no longer needed for the purposes for which it was obtained. Disposition will include (1) the shredding of any hard copies of any Division data, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the service agreement authorizes provider to maintain Division data obtained under the service agreement beyond the time reasonably needed to complete the disposition. Provider shall provide written notification when the division data has been disposed. The duty to dispose of Division data shall not extend to data that has been de-identified or placed in a separate student account, pursuant to the terms of the agreement. The division may employ a request for return or deletion of Division data form, a copy of which is attached hereto as exhibit D. Upon receipt of a request from the division, the provider will immediately provide the division with any specified portion of the division data within ten (10) calendar days of the receipt of said request.
 - a) **Partial Disposal During the Term of Service Agreement**. Throughout the term of the service agreement, Division may request partial disposal of Division data obtained under the service agreement that is no longer needed. Partial disposal of data shall be subject to Division's request to transfer data to a separate account, pursuant to Article II Section 3, above.
 - b) **Complete Disposal upon Termination of Service Agreement**. Upon termination of the service agreement Provider shall dispose or securely destroy all Division data obtained under the service agreement. Prior to the disposal of the data, Provider shall notify Division in writing of its option to transfer data to a separate account, pursuant to Article 2, Section 3, above. In new event shelters Provider dispose of data pursuant to this provision unless and until provider has received affirmative written confirmation from Division that data will not be transferred to a separate account.
6. **Advertising Prohibition**. Provider is prohibited from using or selling Division Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the Division Data for the development of commercial products or services, other than as necessary to provide the Service to the Client. This section does not prohibit Provider from generating legitimate personalized learning recommendations or other

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

activities permitted under Code of Virginia § 22.1-289.01.

7. **Penalties.** The failure to comply with the requirements of this agreement could subject Provider and any third party to all allowable penalties assessable against Provider under state and federal law. In the event the Family Policy Compliance Office of the U.S. Department of Education determines that Provider improperly disclosed personally identifiable information obtained from the Division's education records, the Division may not allow Provider access to the Division's education records for at least five years.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information and makes use of appropriate administrative, technological, and physical safeguards. The general security duties of Provider are set forth below. These duties shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure and manage usernames, passwords, and any other means of gaining access to the Services or to Division Data, at levels suggested by NIST SP800-171 (Password complexity, encryption, and re-use), NIST SP800-53 (IA control Family), and NIST 800-63-3 (Digital Identity), and NIST SP800-63B (Authenticator and Verifier Requirements) or equivalent industry best practices.
 - b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the collection, storage or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment.
 - c. **Provider Employee Training.** The Provider shall provide annual security training to those of its employees who operate or have access to the system.
 - d. **Security Technology.** When the service is accessed using a supported web browser, FIPS 140-2 validated transmission encryption protocols, or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall follow National Institute of Standards and Technology (NIST) 800-171, or equivalent industry best practices.
 - e. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon Division's written request, Service Provider shall make the results of findings available to the Division. The Division shall treat such audit reports as Provider's Confidential Information under this Agreement.
 - f. **Backups and Audit Trails, Data Authenticity and Integrity.** Provider will take reasonable measures, including all backups and audit trails, to protect Division Data against deterioration or degradation of data quality and authenticity. Provider shall be responsible for ensuring that Division Data is retrievable in a reasonable format.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Division Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
- 2. Unauthorized Access or Data Breach.** In the event that Division Data are reasonably believed by the Provider or school division to have been disclosed (lost, accessed or obtained) in violation of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) or other federal or state law applicable to such information accessed or obtained by an unauthorized individual, Provider shall follow the following process:
- a. provide immediate notification to Division upon verification of the incident and allow the Division or its authorized representatives to fully participate in the investigation of the incident.
 - b. notification will be provided to the contact(s) identified in ARTICLE VII, N: Notice, and sent via email and postal mail. Such notification shall include:
 - i. date, estimated date, or date range of the loss or disclosure;
 - ii. Division data that was or is reasonably believed to have been lost or disclosed;
 - iii. remedial measures taken or planned in response to the loss or disclosure.
 - c. immediately take action to prevent further access;
 - d. take all legally required, reasonable, and customary measures in working with Division to remediate the breach, which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the loss or disclosure;
 - e. cooperate with Division efforts to communicate to affected parties;
 - f. provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by Division. If Division requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by Division, Provider shall reimburse Division for costs incurred to notify parents/families of a breach not originating from Division's use of the Service;
 - g. the Provider shall indemnify and hold harmless the Division from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Provider or any of its officers, directors, employees, agents or representatives of the obligations of the Provider's or its Authorized Representatives under this provision or under a Confidentiality Agreement, as the case may be.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

The Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other Division who signs the acceptance in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

- A. Term.** The Provider shall be bound by this DPA for so long as the Provider maintains or possesses any Division data.
- B. Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated. The Division may terminate the DPA and any service agreement or contract in the event of a material breach of the terms of this DPA.
- C. Data Transfer Upon Termination or Expiration.** Provider will notify the Division of impending cessation of its business and any contingency plans. Provider shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the Division. As mutually agreed upon and as applicable, Provider will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the Division, all such work to be coordinated and performed in advance of the formal, transition date.
- D. Effect of Termination Survival.** If the DPA is terminated, the Provider shall destroy all of Division's data pursuant to Article V, section 5(b). The Provider's obligations under this agreement shall survive termination of this Agreement until all Division Data has been returned or Securely Destroyed.
- E. Priority of Agreements.** This DPA supersedes all end user and "click-thru" agreements. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.
- F. Amendments:** This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties
- G. Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
- H. Governing Law: Venue and Jurisdiction.** This agreement will be governed by and

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

construed in accordance with the laws of the state of Virginia, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county of the initial subscribing division or the division specified in Exhibit "E" as applicable, for any dispute arising out of or relating to this agreement or the transactions contemplated hereby.

- I. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Division Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Division Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Division Data and portion thereof stored, maintained or used in any way.
- J. **Waiver.** No delay or omission of the Division to exercise any right hereunder shall be construed as a waiver of any such right and the Division reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
- K. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.
- L. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Virginia and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their hand written signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature.
- M. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the Provider for this Agreement is:

Name: Stephanie Carver
Title: Corporate Counsel and Data Protection Officer
Address: 6625 W 78th Street, ste 220, Bloomington, MN
eMail: privacy@renaissance.com
Phone: (800) 338-4204

The designated representative for the Division for this Agreement is:

Name: Charles Odum
Title: Technology Supervisor
Address: 1570 West Reservoir Street, Wytheville, VA 24382

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

eMail: codum@wythek12.org
Phone: 276-228-5411

- b. Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit “E” General Offer of Terms, subscribing Division shall provide notice of such acceptance in writing and given by personal delivery or email transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below the designated representative for the notice of acceptance of the general offer of privacy terms is named title contact information.

Name: Dana Ziegler
Title: Contract Administrator
Address: PO Box 8036, Wisconsin Rapids, WI 54495
eMail: contracts@renaissance.com
Phone: (800) 338-4204

[Signature Page Follows]

1570 West Reservoir Street, Wytheville, VA 24382

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

IN WITNESS WHEREOF, the parties have executed this Virginia Student Data Privacy Agreement as of the last day noted below.

Provider Signature 
Date: 3/30/2022 Printed Name: Scott Johnson Title: Dir. Information Secur

Division Signature 
Date: March 29, 2022 Printed Name: Charles Odum Title: Technology Supervisor

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

EXHIBIT “A”

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

Renaissance Accelerated Reader is an independent reading practice program that helps K–12 students to become confident, lifelong readers.

Freckle is an adaptive practice program that helps educators to effectively differentiate math, ELA, science, and social studies.

myIGDIs for Preschool are curriculum-based measures that assess the developing literacy, numeracy, and social-emotional skills of pre-K children.

myON is a digital reading platform that provides students with 24/7 access to thousands of fiction and nonfiction books and news articles—in English, Spanish, and additional languages.

Schoolzilla’s data-driven dashboards give educators actionable insights into trends in student attendance and achievement, helping them to identify opportunities to improve outcomes for all learners.

Renaissance Star Assessments are an award-winning suite of valid, reliable assessments for reading, math, and early literacy, in both English and Spanish.

Lalilo is an innovative, visually engaging, standards-aligned literacy software program for grades K–2. It supports literacy learning and instruction through interactive and developmentally appropriate exercises for students and extensive data tracking and planning tools for teachers.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

EXHIBIT “B” SCHEDULE OF DATA

Please refer to the attached Data Elements Collected by Product for this information.

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information- Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information- Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
Schedule	Student scheduled courses Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/ foster care)	
	Other indicator information- Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID	

	number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/appli- cation performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student	

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

	work data - Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

	Other transportation data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

No Student Data Collected at this time _____.
 *Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box, if more space needed.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

EXHIBIT “C” DEFINITIONS

Data Breach means an event in which Division Data is exposed to unauthorized disclosure, access, alteration or use.

Division Data includes all business, employment, operational and Personally Identifiable Information that Division provides to Provider and that is not intentionally made generally available by the Division on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student, employees, and personnel data, user generated content and metadata but specifically excludes Provider Data (as defined in the Contract).

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. Anonymization or de-identification should follow guidance equivalent to that provided by U.S Department of Education publication “Data De-identification: An Overview of Basic Terms” or NISTIR Special Publication (SP) 8053 De-Identification of Personally Identifiable Information. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de- identified if there are fewer than twenty (20) students in the samples of a particular field or category, *i.e.*, twenty students in a particular grade or less than twenty students with a particular disability.

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, staff data, parent data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by Division or its users, students, or students’ parents/guardians, including “directory information” as defined by §22.1-287.1 of the Code of Virginia“.

PII includes, without limitation, at least the following:

- Staff, Student or Parent First, Middle and Last Name
- Staff, Student or Parent Telephone Number(s)
- Discipline Records
- Special Education Data
- Grades
- Criminal Records

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

- Health Records
- Biometric Information
- Socioeconomic Information
- Political Affiliations
- Text Messages
- Student Identifiers Photos
- Videos
- Grade
- Home Address Subject
- Email Address
- Test Results
- Juvenile Dependency Records Evaluations
- Medical Records
- Social Security Number
- Disabilities
- Food Purchases
- Religious Information Documents
- Search Activity
- Voice Recordings
- Date of Birth
- Classes
- Information in the Student's Educational Record
- Information in the Student's Email

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by Division and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational Division employee.

Securely Destroy: Securely Destroy means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards of Technology (NIST) SP 800-88 Appendix A guidelines relevant to sanitization of data categorized as high security. All attempts to overwrite magnetic data for this purpose must utilize DOD approved methodologies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by Division or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information.

Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Virginia and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services. Anonymization or de-identification should guidance equivalent to that provided by U.S Department of Education publication "Data De-identification: An Overview of Basic Terms" or NISTIR Special Publication (SP) 8053 De-Identification of Personally Identifiable Information.

Student Generated Content: Alternatively known as user-created content (UCC), is any form of content, such as images, videos, text and audio, that have been created and posted by student users on online platforms.

Subscribing Division: A Division that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Division or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Third Party: The term "Third Party" means an entity that is not the Provider or Division.

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

EXHIBIT "D" **DIRECTIVE FOR DISPOSITION OF DATA**

[Name or Division or Division] directs [Name of Company] to dispose of data obtained by Provider pursuant to the terms of the DPA between Division and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

- Disposition is Complete. Disposition extends to all categories of data.
 Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:
[Insert categories of data]

2. Nature of Disposition

- Disposition shall be by destruction or secure deletion of data.
 Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date: As soon as commercially practicable

By Insert Date

4. Signature of Authorized Representative of Division

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

5. Verification of Disposition of Data

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

VIRGINIA SCHOOL DATA PRIVACY AGREEMENT

OPTIONAL: EXHIBIT “E” GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the Division to any other school division (“Subscribing Division”) who accepts this General Offer through its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing Division filled on the next page for the Subscribing Division. This General Offer shall extend only to privacy protections and Provider’s signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing Division may also agree to change the data provided by Division to the Provider to suit the unique needs of the Subscribing Division. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or (3) after three years from the date of Provider’s signature to this form. Provider shall notify the Division in the event of any withdrawal so that this information may be transmitted to the Subscribing Divisions.

BY:  _____
Printed Name: Scott Johnson

Date: 3/30/2022
Title/Position: Dir. Information Secu

2. Subscribing Division

A Subscribing Division, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing Division’s individual information is contained on the next page. The Subscribing Division and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____
Printed Name: _____

Date: _____
Title/Position _____

TO ACCEPT THE GENERAL OFFER THE SUBSCRIBING DIVISION MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

BY: _____
Printed Name: Dana Ziegler
Email Address: contracts@renaissance.com

Date: 3/30/2022
Title/Position: Contract Administratc

RENAISSANCE

US Privacy Notice: Renaissance Products

Welcome, Educators! Renaissance Learning, Inc. and its subsidiaries (“Renaissance,” “We,” “Us,” “Our”) are committed to the privacy and security of Your Data. We have created this Privacy Notice to inform You about Your data rights and the measures We take to protect Your Data and keep it private when You are using our Products in the United States.

If You are using Renaissance Products outside of the United States, please find Your applicable Privacy Notice [HERE](#).

Definitions

Capitalized words have special meaning and are defined below.

“Educators,” “You,” “Your” means the district, school or institution contracting with Renaissance for use of the Renaissance Products. If You are an individual serving California students, additional information regarding Your California Consumer Privacy Act rights can be found [HERE](#).

“Authorized User(s)” means Your faculty, staff (including administrators and teachers), students accounted for in Your quote, and the parents of such students.

“Products” means the commercial educational online software products being provided to You under Your Terms of Service & License Agreement. Our products include: Accelerated Reader, Accelerated Math, Star Assessments, Star 360, Star Reading, Star Early Literacy, Star Math, Star Custom, Star CBM, Freckle, myON, Lalilo, myIGDIS, and Schoolzilla.

“Data Protection Legislation” means the Family Educational Rights and Privacy Act (“FERPA”), the Children’s Online Privacy Protection Act (“COPPA”) and any other applicable state education privacy laws and regulations specific to Your Data. If Your School is subject to the California Consumer Privacy Act (“CCPA”), Renaissance acts as a “service provider” as defined under CCPA.

“Your Data” includes: (i) Authorized User rostering information; (ii) Authorized User information or content generated within the Products (ex, scores, assessments, assignments, essays, notes) including, solely with respect to the Star CBM and Lalilo Products, fluency proficiency voice recordings which can be optionally collected by Educators; (iii) Authorized User sign-on information; (iv) student information that You send to Us in connection with a research study request; (v) feedback Your teachers share with Us. Your Data includes both “personally identifiable information” and “personal information” as defined in the applicable Data Protection Legislation. Renaissance considers Your Data to include any information that can be used on its own or with other information to identify Your Authorized Users as individuals.

“De-identified Data” is data that has had any personally identifiable information removed to such a degree that there is no reasonable basis to believe that the remaining data can be used to identify an individual.

Information We Collect

We gather the various types of information below:

- **Usage Information:** We keep track of activity in relation to how You and/or Your Authorized Users use the Products including traffic, location, logs and other communication data.

- **Device Information:** We log information about You and/or Your Authorized User's computing device when they use the Products including the device's unique device identifier, IP address, browser, operating system, and mobile network.
- **Information collected by Cookies and other similar technologies:** We use various technologies to collect aggregated user information which may include saving cookies to Authorized User's computers.
- **Stored Information and Files:** The Products may access files, including metadata, stored on Authorized Users' computing devices if You choose to send or provide to Us.
- **Information Input by You or Authorized Users:** We receive and store information You or Your Authorized Users input into the Products. The specific input information that is stored by each Application can be found [HERE](#).
- **Information Generated from using the Products:** We store information generated by Authorized User's use of the Products. The specific user generated information that is stored by each Application can be found [HERE](#).

How We Use Information

We take Your privacy seriously. Truly. We are proud signatories to the [Student Privacy Pledge](#) which is a voluntary standard that is legally enforceable by the Federal Trade Commission. We won't use Your Data to do anything other than what We describe below. We use Your Data as follows:

- Provide You and Your Authorized Users with access to the Products
- Communicate with Authorized Users as necessary to meet Our obligations to You
- Provide marketing communications to Educators
- Provide You notices about Your account, including expiration and renewal notices
- Carry out Our obligations and enforce Our rights arising from Our Terms of Service and License Agreement
- Notify You of changes to any Products
- Estimate Your size and usage patterns
- Store information about Your preferences, allowing Us to customize Your services
- Maintain and improve performance or functionality of the Products
- Demonstrate the effectiveness of the Products
- To De-identify Your Data so that De-identified Data can be used as follows:
 - aggregate reporting and analytics purposes
 - general research and the development of new technologies
 - improving educational products
 - developing and improving educational sites, services and products
 - where applicable, to support any of the uses above or any other legitimate business purpose



How We Share Information

The security and privacy of Your Data is Our number one priority. We are in the business of making sure You can leverage Your Data to help students. We are not in the business of selling data. We may share and disclose Your Data in the following limited circumstances:

- **Vendors:** We may share Your Data with third party vendors, consultants and other service providers who We employ to perform tasks on Our behalf. These vendors are bound by contractual obligations to keep Your Data safe and honor Our privacy commitments to You. A list of Our hosting and data center vendors can be found [HERE](#).
- **Change of Control:** We are committed to protecting Your Data and honoring Our privacy commitments to You, even in the case We join forces with another organization. If a third-party purchases most of Our ownership interests or assets, or We merge with another organization, it is possible We would need to disclose Your Data to the other organization following the transaction in order to continue providing services to You. The new controlling organization will be subject to the same commitments as set forth in this Privacy Notice.

- **National Security or Law Enforcement:** Under certain circumstances, We may be required to disclose Your Data in response to valid requests by public authorities, including to meet national security or law enforcement requirements.
- **Protection:** We may disclose Your Data if We believe a disclosure is necessary to protect Us, You and/or Your Authorized Users including to protect the safety of a child and/or Our Products.
- **Research:** We may share De-Identified Data with educational institutions; applicable governmental departments or entities working under their authority, to support alignment studies and educational research.
- **Third Parties You Authorize:** We may share Your Data with third parties that You have authorized.

Security

Your Data is stored on servers in the United States with the exception of the Lalilo product which is stored on servers in France. To better serve our US customers, Renaissance anticipates adding a US-based Amazon Web Services region dedicated to our US Lalilo customers within 2021.

The security of Your Data is of the utmost importance to Us. Please review Our [Information Security Overview](#) for more information about how We protect Your Data.

Data Retention and Destruction

We would hate to lose You as a customer, but if You decide not to renew or You terminate Your Terms of Service and License Agreement with Us, We will remove Your Data from the Products.

Contractual Customers: When Your Terms of Service and License Agreement is up for renewal, We provide You with a 60 day grace period prior to scheduling Your Data for removal. If You are using our Freckle Product, You have the option to transfer to our Freckle Product Free-Version prior to having Your Data removed. We provide these options to ensure We will be able to restore access to Your Data should there be a lapse in time between Your contractual end date and Your renewal processing. Following the 60 day grace period, Your Data will be removed from Our primary data storage within 30 days and Our backups within 90 days.

Freckle Product Free-Version: If You are using the Free-Version of Our Freckle product, We will remove accounts that have been consistently inactive for a period of 13 months. Prior to scheduling Your Data for removal, We will send an email to notify You. If You do not wish for Your account to be removed, please respond within 15 days. If We do not hear back from You within that time period, Your Data will be scheduled for deletion and will be removed from Our primary data storage within 30 days and Our backups within 90 days.

If any applicable laws or regulations require Us to keep any of Your Data, We will only keep it for the period and purpose such law or regulation requires.

We do keep, combine and continue to use De-identified Data or anonymized data across all of Our Products.

Privacy Rights

Your Data is, and always will remain, Your property and under Your control. We won't delete, change or divulge any of Your Data except as described in this Privacy Notice.

You are responsible for the content of Your Data. You can retrieve an Authorized User's information using the Products' dashboard(s). If You receive a request from a student or a parent/guardian to change or delete any Authorized User data, You can make the changes to the source data within Your systems.

The Products refresh data on a regular basis. If We are contacted by students, parents or guardians to request data changes or deletions, We will direct their inquiries to You and abide by Your direction.

Data Protection Legislation

Renaissance complies with all applicable Data Protection Legislation. Applicable Data Protection Legislation will control if there is a conflict with this Privacy Notice.

As a condition of using the Products, You are responsible for informing Your Authorized Users about this Privacy Notice and obtaining any applicable parental consents as required by applicable Data Protection Legislation.

Your Nevada Privacy Rights

Senate Bill No. 220 (May 29, 2019) amends Chapter 603A of the Nevada Revised Statutes to permit a Nevada consumer to direct an operator of an Internet website or online service to refrain from making any sale of any covered information the operator has collected or will collect about that consumer. You may submit a request pursuant to this directive by emailing Us at privacy@renaissance.com. We will provide further information about how We verify the authenticity of the request and Your identity. Once again, We are not in the business of selling data. We are required by law to inform our Nevada customers of their important Nevada-specific privacy rights.

Third Parties

The Products may operate with third-party software and/or services obtained separately by You and authorized by You and/or You may be able to access third-party websites and applications (collectively and individually, "Third Party Services"). While We configure Our Products to work with Third Party Services, We do not endorse and are not responsible for the privacy policies, functionality, or operation of Third Party Services.

Updates

If it becomes necessary for Us to change this Privacy Notice, We will post the changes on Our website and do Our best to bring it to Your attention. If that happens, please make sure You review those changes. However, if any laws or regulations change, We will update this Privacy Notice so that We comply with such changes without prior notice. We won't make any material changes to how We use Your Data without notifying You.

Contact Us

If You have any questions or concerns regarding this Privacy Notice, please send a detailed message to privacy@renaissance.com or by mail to Renaissance Learning, Inc., Attn: "Privacy: Data Protection Officer", 6625 W 78th St, Suite 220, Bloomington, MN 55439.

RENAISSANCE

Information Security Overview

Welcome educators! As a leading provider of technology products to K–12 schools worldwide, security is a critical aspect of Renaissance’s business. Renaissance is subject to global data privacy & security regulations including FERPA, COPPA, HIPAA, GDPR, PIPEDA, the Australian Privacy Act, and United States state-specific educational privacy laws. We abide by our regulatory obligations and we strive to exceed the security expectations of the educators we serve. Every day, millions of users depend upon our commitment to protect their data. We take this commitment seriously.

This Information Security Overview describes the ways in which we protect and secure your data. If you are interested in learning more about how we handle the privacy of your data (data use, collection, disclosure, deletion) please visit our [Privacy Hub](#) for more information.

Technical Controls

Data Storage & Hosting

Renaissance Growth Platform, Freckle, myON, Schoolzilla & Lalilo: Renaissance cloud products are secure, durable technology platforms designed around the core pillars of confidentiality, integrity, and availability. Renaissance products are developed, tested, and deployed in Amazon Web Services (AWS) across several geographically and logically separated locations. The AWS cloud, which complies with an array of industry recognized standards including ISO 27001 and SOC 2. AWS provides Renaissance with Infrastructure as a service (IaaS) through servers, networking, storage, and databases. For more information about AWS, please visit <https://aws.amazon.com/about-aws/global-infrastructure/>.

Renaissance Data Center & Legacy Products: The Renaissance Data Center is our self-hosting data center located in our headquarters in Wisconsin Rapids, WI. The Renaissance hosted data management platform is a closed system. This means that the secure web-based servers, storage, and databases that support the Renaissance hosted platform are dedicated hardware that is used only for that purpose. Each customer’s data is stored in a separate directory and database that operates independently of all other customers’ directories and databases. Each school or district that uses our products has its own unique Renaissance hosted site URL, and each user is assigned unique login credentials, which must be authenticated before the user can access the corresponding Renaissance hosted site.

Data Location

Renaissance Growth Platform, Freckle, Schoolzilla & Renaissance Data Center: Your data is stored on servers in the United States.

myON: Your data is stored on servers based on your geographic location.

- US Customers: Your data is stored on servers in the United States.
- European Customers: Your data is stored on servers in the United Kingdom
- Australia, New Zealand, and Asia-Pacific Customers: Your data is stored on servers in Singapore

Lalilo: Your data is stored on servers in France. In order to better serve our US customers, Lalilo by Renaissance anticipates adding a US-based Amazon Web Services region dedicated to our US customers within 2021.

Encryption

Customer data hosted within our Renaissance products is encrypted in transit and at rest.

All server-to-client access of Renaissance applications and data requires HTTP over Transport Layer Security (TLS), also known as HTTPS (Port 443). TLS provides privacy, integrity, and protection for data that is transmitted between different nodes on the Internet, and it prevents data from being eavesdropped or tampered with in transit. We use 256-bit AES encryption with 2048-bit keys to further ensure the Internet traffic between Renaissance and our customers cannot be intercepted.

Our optional Renaissance data integration service automatically refreshes the district's Renaissance applications daily with new data from the student information system. It transfers data over a secure FTP connection (Port 22) for automated extracts and uses a Secure Sockets Layer (SSL)/HTTPS (Port 443) connection when data is uploaded or entered through the software.

Passwords and Role-Based Access

Each school or district has a unique URL to access its Renaissance products. Each user is assigned unique login credentials, which must be authenticated before the user can access the school or district site. Users are assigned to distinct roles, such as student, teacher, or administrator, which limits what information users can access or edit.

Network Security Features

Vigorous network security procedures protect customers' data from electronic intrusion. These include antivirus software; firewalls; regular patching, updating, and hardening processes; and application security to ensure connectivity protection. Renaissance performs full-system scans on a regular schedule and updates antivirus signatures as they are released. Renaissance tracks an array of metrics, including log files, access logs, system usage, and network bandwidth consumption. We monitor all hosted systems 24 hours a day, 7 days a week, using various methods. Any suspicious activity is promptly investigated and addressed. A protective monitoring regime tracks how our information and communications technology systems are used. We also protect these systems from malicious and mobile code. Network security boundaries, also known as segmentation, are defined and enforced to limit access to customer data.

Application Security Testing

Dynamic Application Security Testing (DAST) are run against all our applications on a regular basis. The DAST process, which is an integral piece of our software development cycle, tests our software for exploitable weaknesses and vulnerabilities at each stage of the development process. Vulnerability scans also run on a regular basis. These scans are used to identify and remediate vulnerabilities that may be present in our hosting and corporate platforms.

Business Continuity & Disaster Recovery

We follow stringent data backup and recovery protocols to protect our customer data. Renaissance uses a combination of both full and incremental backups to assist with recovery scenarios. Backups are encrypted and sent off site to redundant storage. Services are deployed via Docker containers and load balanced across hosts running in multiple availability zones to provide high availability and mitigate the risk of service outage. Renaissance also manages much of its cloud infrastructure as code, which facilitates quick recovery or rollback in case of outage, and better transparency into changes in infrastructure over time.

In the event of complete outage, our recovery objectives are to have full functionality within 24 hours, with no more than 1 hour of user data lost.

Physical Controls

Renaissance Growth Platform, Freckle, myON, Schoolzilla & Lalilo: Renaissance cloud products are powered by AWS, a secure, durable technology platform that aligns to an array of industry-recognized standards. Its services and data centers have multiple layers of operational and physical security. For more information about AWS, please visit <https://aws.amazon.com/about-aws/global-infrastructure/>

Renaissance Data Center & Legacy Products: The primary location of Renaissance's key systems—including the primary data center—is within the Wisconsin Rapids, Wisconsin, corporate headquarters. Entry into Renaissance's corporate headquarters, which houses the primary data center, is controlled via employee magnetic key entry.

Only hosting services department and information system employees who are responsible for the entire corporate infrastructure are allowed unescorted access to the Renaissance data center. Admittance to the data center itself is controlled through a proximity card access system and a motion-based detection system. All visitors to the data center, as well as their internal employee escorts, must sign an access log. We also monitor log files, review access logs, track system usage, and monitoring network bandwidth consumption.

A second environmentally controlled systems room located within Renaissance's Wisconsin Rapids headquarters houses corporate technology and redundant systems for the corporate data center. This area also is restricted to Renaissance network services employees, and entrance also is monitored by a proximity key.

The environmental conditions within the data center are maintained at a consistent temperature and humidity range, and a third-party security firm monitors conditions within the data center. Should any changes in power or temperature occur, key Renaissance personnel are notified. Electrical power is filtered and controlled by dual uninterruptible power systems. If a power outage occurs, an automatic generator provides uninterrupted power to our servers and heating, ventilation, and air conditioning units. A backup generator sustains longer-term operations. A waterless fire protection system and an early-warning water detection system help to prevent damage to the servers that store our customers' data.

Administrative Controls

Risk Management Approach

Our security processes and controls substantially follow the **National Institute of Standards and Technology's Federal Information Processing Standards (FIPS) 200 standard** and related **NIST Special Publication 800-53**. Renaissance also assesses its Information Security and Privacy programs against the CIS Top 20 Controls and the NIST Cybersecurity Framework (CSF).

Cybersecurity Risk Committee: The Renaissance Cybersecurity Risk Committee is charged with identifying, tracking, and managing risks. The committee communicates with executive leadership and the board of directors to keep them informed of key cyber and business level risks facing Renaissance. The committee assesses all observed and perceived risk to develop policy, practices, and priorities to manage risk to an acceptable level.

Governance

Information Security & Privacy Committee: Our risk management plan allows our company to remain up to date on information including security best practices, government policy and legislation, threats and vulnerabilities, and new technologies. Our risk management plan is informed by the Information Security & Privacy Committee which is charged with evaluating our Renaissance information security and privacy policies, procedures, and operations along with Renaissance's products, product development, and product deployment systems to identify potential

areas of vulnerability and risk. These evaluations are used to develop policy, practices, and processes aimed at mitigating or removing vulnerability and risk. Evaluations also inform strategic direction for information security and privacy programs. The Information Security & Privacy Committee reports to the Executive Leadership Team.

Application Security Guild: The Renaissance Application Security Guild is a group of security practitioners, enthusiasts, and learners from across the organization who focus their efforts on creating a culture of secure application development, developing tactical-level guidance, evangelizing best practices, and providing training. The Renaissance Application Security Guild meets every month to share knowledge, learning materials, technologies, and development patterns to be used as inputs to other security practices and processes.

Incident Response Team

Renaissance maintains an Incident Response Plan. Renaissance's employees and agents are obligated to protect all customer data and ensure its security. This includes immediately reporting any suspected or known security breaches, theft, unauthorized release, or unauthorized interception of customer data

Our proactive risk management plan allows our company to stay up to date on information including security best practices, government policy and legislation, threats and vulnerabilities, and new technologies. However, should evidence of intrusion or unauthorized access arise, our Incident Response team will execute the following countermeasures:

1. Sever the connection of the intruder to the compromised system(s), including but not limited to restricting IP addresses, disabling services, and powering off the Renaissance virtual server.
2. Activate the Incident Response Plan.
3. Assess the damage from the intrusion.
4. Assess the intrusion and correcting security vulnerabilities.
5. Report assessment, damage, and remedies to the data owner.

Upon confirmation of a data breach, Renaissance's Data Protection Officer would notify the district's designated contact within the applicable regulatory or contractually agreed upon timelines. This e-mail will include the date and time of the breach, the names of the student(s) whose data was released, disclosed, or acquired (to the extent known); the nature and extent of the breach, and Renaissance's proposed plan to investigate and remediate the breach.

Renaissance will investigate and restore the integrity of its data systems. Within 30 days after discovering a breach, Renaissance will provide the district's designated contact with a more detailed notice of the breach, including but not limited to the date and time of the breach; name(s) of the student(s) whose student data was released, disclosed or acquired; nature of and extent of the breach; and measures taken to prevent a future occurrence.

We encourage district representatives with any questions or concerns regarding privacy, security, or related issues to contact our Data Protection Officer via e-mail at privacy@renaissance.com.

Security Education, Training & Awareness

All Renaissance employees are required to complete 1.5 hours of both Global Privacy and Information Security training on annual basis.

Renaissance conducts a regular anti-phishing awareness program. The Information Security team sends batches of simulated phishing email “tests” to all employees on a monthly basis. The Information Security team reports on these metrics as a Key Performance Indicator.

Renaissance regularly communicates cybersecurity information relevant to the current threat environment to all employees.

Compliance

Employees: All Renaissance employees and contractors must sign a legally enforceable nondisclosure agreement prior to the start of their employment or contract. They are additionally required to read, sign and agree to abide by Renaissance’s technology policies. Employees and contractors must clear a background check before starting their employment or contract.

Vendors: Renaissance maintains a vendor compliance program. Renaissance has invested in privacy compliance management software whereby vendor data is inventoried, assessed and mapped. Vendors’ security and privacy practices are reviewed and evaluated. Renaissance vendors are contractually bound to comply with the security and privacy requirements of both Renaissance and our customers.

If you have specific information security questions, please contact: infosecurity@renaissance.com

Data Elements: Collected by Product

Data Category	Data Elements	Star Assessments	Star Early Literacy	Accelerated Reader	Accelerated Math	myON	Freckle	myIGDIs	Schoolzilla	Schoolzilla Starter	Lalilo
Application Technology Metadata	IP Addresses of users, use of cookies, etc.	Required	Required	Required	Required	Required	Required		Required	Required	Required
	Other application technology metadata	Required	Required	Required	Required	Required	Required		Required	Required	Required
Application Use Statistics	Metadata on user interaction with application	Required	Required	Required	Required	Required	Required		Required	Required	Required
Assessment	Standardized test scores	Optional					Optional		Optional		
	Observation data	Optional (Star CBM-US Only)						Required	Optional		
	Testing Environment	Required (US) Optional (UK)	Required (US) Optional (UK)								
	Voice Recordings	Optional (Star CBM-US Only)									Optional
	Other Assessment Data					Optional	Optional		Optional		
Attendance	Student school (daily) attendance data								Optional		
	Student class attendance data								Optional		
Communication	Online communications that are captured (emails, blog entries)					Optional					

RENAISSANCE

Demographics	Conduct or behavioral data								Optional		
	Date of Birth	Optional	Required	Optional	Optional			Required	Optional	Optional	
	Place of Birth								Optional		
	Gender	Optional	Optional	Optional	Optional			Required	Optional	Optional	
	Ethnicity or race	Optional	Optional	Optional	Optional				Optional	Optional	
	Specialized education services (IEP or 504)	Optional	Optional	Optional	Optional			Optional	Optional	Optional	
	Living situations (homeless/foster care)	Optional	Optional	Optional	Optional				Optional	Optional	
	Language information (native, preferred or primary language spoken by student)	Optional	Optional	Optional	Optional				Optional	Optional	Optional
	Other indicator information								Optional		
Enrollment	Student school enrollment	Required									
	Student grade level	Required	Required	Required	Required	Optional	Required	Required	Required	Required	Required
	Homeroom							Required	Optional		Required
	Guidance counselor								Optional		
	Specific curriculum programs								Optional		
	Year of graduation								Optional		
	Other enrollment information										
Parent/Guardian Information	Address								Optional		
	Email	Optional	Optional	Optional	Optional				Optional	Optional	Optional
	Phone								Optional		
	First and/or Last			Optional					Optional		

RENAISSANCE

Schedule	Student scheduled courses	Required	Required	Required	Required				Optional	Required	Required
	Teacher names	Required	Optional	Required	Required						
	Teacher emails	Required	Optional	Required	Required						
Special Indicator	English language learner information	Optional	Optional	Optional	Optional			Optional	Optional	Optional	
	Low income status - SES Free and Reduced	Optional	Optional	Optional	Optional			Optional	Optional	Optional	
	Medical alerts/health data										
	Student disability information	Optional	Optional	Optional	Optional			Optional	Optional	Optional	
Student Contact Information	Address								Optional		
	Email								Optional		
	Phone								Optional		
Student Identifiers	Local (School district) ID number	Optional	Optional	Optional	Optional	Required	Optional	Required	Required	Optional	Optional
	Vendor/App assigned student ID number	Required	Required	Required	Required	Required			Required	Required	Required
	Student app username	Required	Required	Required	Required	Required			Optional		Required
	Student app passwords encrypted only for SSO	Required	Required	Required	Required	Required	Optional			Required	Required
	First and/or Last	Required									
Student In App Performance	Program / application performance (typing program- student types 60 wpm, reading program-student	Required	Required	Required	Required	Required	Required				Required

RENAISSANCE

	reads below grade level)										
Student Survey Responses	Student responses to surveys or questionnaires	Required	Required	Required	Required	Optional	Required	Required			
Student Work	Student generated content; writing, pictures etc.					Optional					
	Other student work data										
Transcript	Student course grades								Optional		
	Student course data								Optional		
	Student course grades/performance scores								Optional		
	Other transcript data								Optional		
Transportation	Other transportation data										