DISCLAIMER for MOREnet's Missouri NDPA

The Student Data Privacy Consortium ("SDPC") has developed the "National Data Privacy Agreement" ("NDPA"). The SDPC formed a DPA Project Team consisting of individuals from schools, state organizations, marketplace providers, and legal organizations to develop this standard template that addresses the common student data privacy issues that need to be addressed in contracts with vendors that handle student data (see https://privacy.a4l.org/national-dpa) .

The Missouri Research and Education Network (MOREnet), a department of the University of Missouri System, has joined the SDPC and has established the Missouri Student Privacy Alliance, which all MOREnet Member schools are eligible to join. As such, MOREnet is making the NDPA available to its members as a resource for informational purposes only; it should not be relied on as legal advice. While MOREnet believes this is a well-developed tool, MOREnet makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in the NDPA. ***Should you elect to use the NDPA as a resource, we strongly encourage you to obtain your own legal counsel in drafting and/or entering into vendor agreements that pertain to student data.*** There may be unique needs of your school or systems that need to be addressed or other provisions that you believe are critical, which can be set forth in Exhibit H.

Exhibit G is intended to include any specific Missouri laws that apply to student data, which may be applicable to your school. However, laws are constantly subject to change and new ones can be enacted. Additionally, there may be other laws or National or Missouri guidelines or standards that are applicable to your school with which you must comply. ***MOREnet is not representing that the laws set forth in Exhibit G are the only laws, guidelines, and/or standards which should be included, as applicable to you and/or to a specific vendor agreement***. Your own legal counsel should be consulted and any additional terms you may require should be added to Exhibit H.

STANDARD STUDENT DATA PRIVACY AGREEMENT

MO-NDPA Standard

Version 1.0

Festus R-VI School District

and

Renaissance Learning Inc

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Festus R-VI School District , located at 1515 Mid Meadow Ln Festus MO 6 (the "**Local Education Agency**" or "**LEA**") and Renaissance Learning Inc , located at (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   ✓ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**

   ☑ If Checked, the Provider, has signed Exhibit "E" to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Joshua L Bauman

Title: Director of Technology

Address:

1515 Mid Meadow Ln Festus, MO 63028

Phone: 6369374920

Email: Baumanjosh@festusedu.com

The designated representative for the Provider for this DPA is:

Name: Stephanie Carver Title: Corporate Counsel & Data Protection Officer

Address:

3325 W 78th Street, Suite 200, Bloomington, MN 55439

Phone: (800) 338-4204

Email: privacy@renaissance.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA Festus R-VI School District

By: _____ Date: 5-16-2022

Printed Name: Joshua L Bauman Title/Position: Director of Technology

Renaissance Learning Inc

By: _____ Date: 5/13/2022

Printed Name: Scott Johnson Title/Position: Dir. Information Security

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA 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 applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-

public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student 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 LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an

appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

   (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

      i. The name and contact information of the reporting LEA subject to this section.
      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
      iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
      v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

   (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized

acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

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 **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. 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. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **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.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **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 In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

As a global leader in assessment, reading, and math solutions for pre-K–12 schools and districts, Renaissance is committed to providing educators with insights and resources to accelerate growth and help all students build a strong foundation for success. Renaissance solutions are used in over one-third of US schools and in more than 90 countries worldwide. The Renaissance portfolio includes Star Assessments, for reliable, accurate insights into K–12 student learning; myIGDIs, for accurate assessment of early learning; myON, to increase students' access to high-quality reading materials; Accelerated Reader, to support independent reading practice; Freckle, for teacher-led differentiated instruction; Lalilo, an innovative, visually engaging, standards-aligned literacy software program for grades K–2; and Schoolzilla, to give educators actionable insights into trends in student attendance and achievement.

Please refer to the attached US Privacy Notice, Information Security Overview, and Data Elements Collected by Product for full details how Renaissance uses and protects your data.

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

EXHIBIT "B"
SCHEDULE OF DATA

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 captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, 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:	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
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/application 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 work data -Please specify:	

Category of Data	Elements	Check if Used by Your System
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:	

Category of Data	Elements	Check if Used by Your System
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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 Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA 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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

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

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

Festus R-VI School District Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ 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 here

_X_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_X_ Disposition shall be by destruction or 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. Schedule of Disposition

Data shall be disposed of by the following date:

_X_ As soon as commercially practicable.

_____ By Insert Date Here

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [Festus R-VI School Distri] ("Originating LEA") which is dated [5/13/2022], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. 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 LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. 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 listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: contracts@rennaissance.com

[Renaissance Learning Inc]

BY: _____ Date: 5/13/2022

Printed Name: Scott Johnson Title/Position: Dir. Information Security

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the [Festus R-VI School District] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G" – Supplemental NDPA State Terms for Missouri

Version: October 2020

A. DATA BREACH

In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student's family member, Provider shall notify LEA within five (5) business days. The notice shall include:

1. Details of the incident, including when it occurred and when it was discovered;
2. The type of personal information that was obtained as a result of the breach; and
3. The contact person for Provider who has more information about the incident.

"*Breach*" shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

"*Personal information*" is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:

1. Social Security Number;
2. Driver's license number or other unique identification number created or collected by a government body;
3. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
4. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account;
5. Medical information; or
6. Health insurance information.

EXHIBIT "H"
Additional Terms or Modifications
Version _____

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

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.

The security of Your Data is of the utmost importance to Us. Please review Our [redacted] 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 [redacted] or by mail to Renaissance Learning, Inc., Attn: "Privacy: Data Protection Officer", 6625 W 78th St, Suite 220, Bloomington, MN 55439.

Effective Date: 31 Jan 2022

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. To better serve our US customers, Renaissance anticipates adding a US-based Amazon Web Services region dedicated to our US Lalilo customers within 2021.

Encryption

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

All client-to-server 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 eavesdropping and tampering during transit. We use 256-bit AES encryption with 2048-bit keys to secure Internet traffic between Renaissance and our customers.

Our optional Renaissance data integration service automatically refreshes the district's Renaissance applications daily with new data from the student information system. This service 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 testing 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) is 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 and 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 into scalable groups and are load balanced across compute and storage 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 is controlled via employee magnetic key entry.

Only Cloud Operations and Network Services personnel who are responsible for management of all cloud 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 Center for Internet Security (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 and has a standing Incident Response Team. The Incident Response Team performs Table Top Exercises twice annually. 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 emails to all employees on a monthly basis. The Information Security team provides additional phishing awareness training and reports on testing 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**

RENAISSANCE

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	Required
Application Use Statistics	Metadata on user interaction with application	Required	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	Optional		
Communication	Online communications that are captured (emails, blog entries)					Optional					
Demographics	Conduct or behavioral data								Optional		
	Date of Birth	Optional	Required	Optional (US)	Optional			Required	Optional	Optional	

RENAISSANCE

				Required (UK)							
	Place of Birth								Optional		
	Gender	Optional	Optional	Optional	Optional			Required	Optional	Optional	
	Ethnicity or race	Optional	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		Required	Optional	Optional	Optional	Optional
	Other indicator information								Optional		
Enrollment	Student school enrollment	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required
	Student grade level	Required	Required	Required	Required	Required	Required	Optional	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		
Schedule	Student scheduled courses	Required	Required	Required	Required				Optional	Required	Required
	Teacher names	Required	Required	Required	Required	Required	Required	Required	Optional	Required	Required

RENAISSANCE

	Teacher emails	Required	Required	Required	Required	Required	Required	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	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	Required	Required	Required	Required	Required	Required	Required	Required	Required
Student In App Performance	Program / application performance (typing program- student types 60 wpm, reading program-student reads below grade level)	Required	Required	Required	Required	Required	Required	Required			Required
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	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										