

CALIFORNIA STUDENT DATA PRIVACY
AGREEMENT Version 2.0 (September 26, 2018)

School District/Local Education Agency:

Twin Rivers Unified School District

AND

Provider:

Renaissance Learning, Inc.

Date:

10/8/2020

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the Twin Rivers Unified School District

(hereinafter referred to as “LEA”) and Renaissance Learning, Inc. (hereinafter referred to as “Provider”) on 10/8/2020 . The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) pursuant to a contract dated (“Service Agreement”); and

10/8/2020

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (“SOPIPA”) found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms 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 LEAs in California 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 student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, 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. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

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

Renaissance assessment and practice solutions

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”.
4. **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 term used in the Service Agreement.

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 Agreement 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 LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA’s request for Student Data 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 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 pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit “A”, Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (4 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 data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected 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 state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise 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 Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **No Disclosure.** De-identified information 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). Provider agrees not to attempt to re-identify de-identified Student Data and 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 LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student 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 Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’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 delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial 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 LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:

- a. Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA’s designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer 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 Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
- f. Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student 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.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

- a. The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - 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.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c. At LEA’s discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to all requirements in applicable State and in federal law 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.

- e. 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 copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA 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 LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. 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 PRIVACY 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 this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .
2. **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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, 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 LEA for this Agreement is:

Name: Barbara Schiffner
Title: Director of IETS

Contact Information:
Barbara.Schiffner@twinriversusd.org
916-566-3400

The designated representative for the Provider for this Agreement is:

Name: Stephanie Carver
Title: Data Protection Officer

Contact Information:
6625 W 78th Street, Suite 220
Bloomington, MN 55439
privacy@renaissance.com

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail 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:

Name: Contracts
Title: Contract Administrator

Contact Information:
PO Box 8036 / 2911 Peach Stree
Wisconsin Rapids, WI 54495
contracts@renaissance.com

6. Entire Agreement. This DPA constitutes 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.

7. **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.
8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **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.

[Signature Page Follows]

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

Provider: Renaissance Learning, Inc.

BY:  Date: 10/8/2020

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

Local Education Agency: Twin Rivers Unified School District

BY:  Date: 10/28/2020

Printed Name: Barbara Schiffner Title/Position: Director of IETS

Note: Electronic signature not permitted.

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 Math is an adaptive program that helps educators effectively differentiate math instruction and practice. Interactive features, team challenges, real-world scenarios, and instant feedback make practice engaging and fun, while embedded supports and scaffolds help students master even the most challenging math concepts.

myIGDIs by Renaissance 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. A multimedia reading experience with colorful illustrations, professionally recorded audio, and annotation tools makes each text engaging and unique.

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. These near real-time dashboards can integrate over 135 education data sources, including student information systems, interim and state tests, Star Assessments, behavior management systems, and more.

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

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.	required
	Other application technology meta data- Please specify:	required
Application Use Statistics	Meta data on user interaction with application	required
Assessment	Standardized test scores	optional
	Observation data	required for myIGIDs
	Other assessment data-Please specify:	optional
Attendance	Student school (daily) attendance data	optional for Schoolzilla
	Student class attendance data	optional for Schoolzilla
Communications	Online communications that are captured (emails, blog entries)	

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

Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
Schedule	Student scheduled courses	required
	Teacher names	required
Special Indicator	English language learner information	optional
	Low income status	optional
	Medical alerts /health data	
	Student disability information	optional
	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	optional

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

	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.

Data Elements: Collected by Product

Data Category	Data Elements	Star Assessments	Star Early Literacy	Accelerated Reader	Accelerated Math	myON	Freckle	myIGDIs	Schoolzilla	Schoolzilla Starter
Application Technology Metadata	IP Addresses of users, use of cookies, etc.	Required	Required	Required	Required	Required	Required		Required	Required
	Other application technology metadata	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
Assessment	Standardized test scores	Optional					Optional		Optional	
	Observation data							Required	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				
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
Other indicator information								Optional		
Enrollment	Student school enrollment	Required	Required	Required	Required	Required	Required	Required	Required	Required
	Student grade level	Required	Required	Required	Required	Optional	Required	Required	Required	Required
	Homeroom							Required	Optional	
	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
	Phone								Optional	
	First and/or Last								Optional	
Schedule	Student scheduled courses	Required	Required	Required	Required				Optional	Required
	Teacher names	Required	Required	Required	Required	Required	Optional	Required	Optional	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
	Vendor/App assigned student ID number	Required	Required	Required	Required	Required			Required	Required
	Student app username	Required	Required	Required	Required	Required	Required		Optional	
	Student app passwords encrypted only for SSO	Required	Required	Required	Required	Required	Optional			Required
	First and/or Last	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			
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									

EXHIBIT “C”

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

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.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Operator: The term “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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term “Operator” is replaced by the term “Provider.” This term shall encompass the term “Third Party,” as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student 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 LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, 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. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

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 LEA 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 LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

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

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

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, 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 California 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.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Subscribing LEA: An LEA 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 LEA 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.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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 pupil records. However, for the purpose of this Agreement, 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

Twin Rivers Unified School District directs Renaissance Learning, Inc. 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:

<p><u>Extent of Disposition</u></p> <p>Disposition shall be:</p>	<p>_____ Partial. The categories of data to be disposed of are as follows:</p> <p>_____ Complete. Disposition extends to all categories of data.</p>
<p><u>Nature of Disposition</u></p> <p>Disposition shall be by:</p>	<p>_____ Destruction or deletion of data.</p> <p>_____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.</p>
<p><u>Timing of Disposition</u></p> <p>Data shall be disposed of by the following date:</p>	<p>_____ As soon as commercially practicable</p> <p>_____ By (Insert Date) _____</p>

Authorized Representative of LEA

Date

10/8/2020

Verification of Disposition of Data
by Authorized Representative of Provider

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 Twin Rivers Unified School and which is dated 10/8/2020 to any other LEA ("Subscribing LEA") who accepts this 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 other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify CETPA in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider: Renaissance Learning, Inc.

BY: 
Printed Name: Scott Johnson

Date: 10/8/2020
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.

Subscribing LEA:

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

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

Name: PO Box 8036 / 2911 Peach Stree

Title: _____

Email Address: _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

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, 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.

“**Your Data**” includes: (i) Authorized User rostering information; (ii) Authorized User information or content generated within the Products (ex, scores, assessments, assignments, essays, notes); (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. 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. The Renaissance Growth Platform is a secure, durable technology platform designed around the core pillars of confidentiality, integrity, and availability. The Renaissance Growth Platform is 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, is dispersed throughout 61 zones worldwide, including 16 zones in the U.S. in California, Ohio, Oregon, and Virginia. 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.

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

Data Location

Your data is stored on servers in the United States.

Encryption

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

All server-to-client access of the Renaissance hosted platform 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: The Renaissance Growth Platform is 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**.

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 through the General Counsel.

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.