



**Arbor Park School District 145
and Renaissance Learning, Inc.**

Data Privacy Addendum (Student Data Only)

This Data Privacy Addendum (the "Addendum") by and between Arbor Park School District 145 (the "School District") and Renaissance Learning, Inc. (the "**Company**") (collectively, the "Parties") is incorporated in, effective simultaneously with, and modifies the attached agreement between the Parties and all current and supplemental terms and conditions, order forms, policies, practices, procedures, and/or other documentation relating to the attached agreement (collectively, the "Agreement"). This Addendum supersedes the Agreement by adding to, deleting from, and modifying the Agreement. To the extent any provision in this Addendum results in any conflict or inconsistency between the Agreement and this Addendum, this Addendum shall govern and any term of the Agreement that conflicts with this Addendum or is inconsistent with this Addendum shall be of no force or effect.

1. Definition of School District Data

As used in this Addendum, "School District Data" includes:

- "Personally Identifiable Information" and "Education Records" of students as defined in regulations implementing the Family Educational Rights and Privacy Act ("FERPA"), 34 C.F.R. § 99.3;
- "School Student Records" as defined in the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/2(d);
- "Covered Information" as defined in the Illinois Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/5; and
- All other non-public information, including student data, metadata, and user content, of the School District's students.

2. Services and Data Provided

2.1 *Nature of Products or Services Provided.* The Company has agreed to provide the following products and/or services to the School District:

Renaissance assessment and practice solutions.

2.2 *School District Data Provided.* To allow the Company to provide the products and/or services described in *Section 2.1*, the School District will provide the following categories or types of School District Data to the Company in Exhibit B.

2/1/21

- 2.3 *Minimum Data Necessary Shared.* The Company attests that the data requested by the Company from the School District for the School District to access the Company's products and/or services represents the minimum necessary data for the products and/or services as described in the Agreement and this Addendum.
- 2.4 *Publication of Agreement and Subcontractors.* Under SOPPA, the School District must publish the Company's name and business address, a copy of the Agreement and this Addendum, and a list of any subcontractors to whom School District Data may be disclosed. The Company agrees to provide to the School District prior to execution of the Agreement and this Addendum the name, business address, and list of subcontractors to be published.

3. Compliance with Law

- 3.1 The Company agrees that all sharing, use, and storage of School District Data will be performed in accordance with all applicable Federal and State laws. The Company agrees that it will comply with all applicable laws and refrain from using School District Data in any way prohibited by any law, whether such requirements are specifically set forth in this Addendum. Applicable laws may include, but are not limited to, FERPA; ISSRA; SOPPA; the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; the Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. 1232 h; and the Illinois Children's Privacy Protection and Parental Empowerment Act ("CPPPEA"), 325 ILCS 17/1 *et seq.*

4. Data Ownership and Use

- 4.1 *Data Ownership and Control.* The School District Data and any intellectual property rights thereto remain the property of and under the control of the School District. The Company does not obtain any right, title, or interest in any of the School District Data furnished by the School District.
- 4.2 *School District Access to Data.* Any School District Data in the possession or under the control of the Company shall be made available to the School District upon request by the School District. The Company shall be responsible to provide copies of or access to School District Data in the possession or under the control of the Company to the School District within a reasonable time frame and in all cases within time frames that will allow timely compliance by the School District with any statutorily or court ordered deadline. This includes requests under the Illinois Freedom of Information Act ("FOIA"), 5 ILCS 140/1 *et seq.*, requests regarding student records under FERPA or ISSRA, requests for records in discovery in state or federal court or administrative proceedings, and any other request.

4.3 *Company Use of Data.* The Company may use and disclose the School District Data only for the purposes described in the Agreement and only in a manner that does not violate local, state, or federal privacy laws and regulations. These include, but are not limited to, the following requirements, as applicable:

4.3.1 School Officials Requirements. The Company acknowledges that it is acting and designated as a "school official" or "official of the school" with a "legitimate educational interest" in the School District Data as those terms are used in FERPA, ISSRA, and SOPPA (a "School Official"). The Company agrees to abide by the limitations and requirements applicable to a School Official. The Company agrees it is performing an institutional service or function for which the school would otherwise use employees and is under the direct control of the school with respect to the use and maintenance of the School District Data. The Company agrees that it will use the School District Data only for authorized purposes and will comply with all limitations and requirements imposed on a School Official under FERPA, ISSRA, and SOPPA, including the requirements that the Company: (1) collect and use School District Data only for the purpose of fulfilling its duties under the Agreement and this Addendum and only for the benefit of the School District and its end users; (2) will not share, disclose, or re-disclose the School District Data to any third party or affiliate except as permitted by FERPA, ISSRA, and SOPPA or provided for in this Addendum, otherwise authorized in writing by the School District, or pursuant to a court order; (3) will not use School District Data (including metadata) for advertising or marketing purposes unless such use is specifically authorized by this Addendum or otherwise authorized in writing by the School District.

4.3.2 PPRA Requirements. With respect to the Company's collection, disclosure, or use of School District Data as governed by the PPRA, the Company's collection, disclosure, or use of any School District Data shall be for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, the School District's students or educational institutions, or otherwise for the use and benefit of the school. The Company will not use the School District Data for any purpose other than the School District's purpose.

4.3.3 COPPA Requirements. To the extent applicable, the Company agrees that its use of the School District Data will be solely for the benefit of the School District's students and for the school system, and that the Company will not collect personal information from students for any purpose other than the School District's purpose, including any other commercial purpose.

4.4 *Internal Company Disclosure.* The Company attests that only individuals or classes of individuals who are essential to perform the work under the Agreement will have access to the School District Data and that those individuals and classes of individuals will be familiar with and bound by this

Addendum and relevant law. The Company shall cause each officer, director, employee, subcontractor, and other representative who will have access to any School District Data during the term of the Agreement to comply with all legal requirements applicable to the School District Data, including but not limited to those outlined in this Agreement and under relevant law.

5. Company Obligations Regarding Data

5.1 *Safeguards.* The Company agrees to take appropriate administrative, technical, and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of School District Data. The Company shall ensure that School District Data are secured and encrypted to the greatest extent practicable during use, storage and/or transmission.

5.1.1 *Security Procedures and Practices.* The Company agrees that at it will implement and maintain security procedures and practices that, at a minimum, are designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure that based on the sensitivity of the data and the risk from unauthorized access: (i) use technologies and methodologies that are consistent with the U.S. Department of Commerce's National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. and any updates to it; or (ii) maintain technical safeguards as they relate to the possession of covered information in a manner consistent with the provisions of 45 C.F.R. 164.312.

5.1.2 *Storage of Data.* The Company agrees to store and process the School District Data in a manner that is no less protective than those methods used to secure the Company's own data. The Company agrees that School District Data will be stored on equipment or systems located within the United States.

5.1.3 *Audit of Safeguards.* The Company shall maintain complete and accurate records of its security measures for School District Data and produce such records to the School District for purposes of audit upon reasonable prior notice during normal business hours. The School District reserves the right at its sole discretion to audit the Company's storage of School District Data at the School District's expense to ensure compliance with the terms of the Agreement and this Addendum.

5.1.4 *Reasonable Methods.* The Company agrees to use "reasonable methods" to ensure to the greatest extent practicable that the Company and all parties accessing School District Data are compliant with state and federal law. The School District reserves the right to audit such measures upon reasonable prior notice during business hours.

5.2 *Privacy Policy.* The Company must publicly disclose material information about its collection, use, and disclosure of covered information, including, but not

limited to, publishing a terms of service agreement, privacy policy, or similar document. Any changes the Company may implement with respect to its privacy policies or terms of use documents shall be ineffective and inapplicable with respect to the School District and/or School District Data unless the School District affirmatively consents in writing to be bound by such changes. Access by students or parents/guardians to the Company's programs or services governed by the Agreement and this Addendum or to any School District Data stored by the Company shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this Addendum.

- 5.3 *Data Return/Destruction.* Upon expiration of the term of the Agreement, upon the earlier termination of the Agreement for any reason, at a time when some or all the School District Data is no longer needed for purposes of the Agreement, or upon the School District's request, the Company covenants and agrees that it promptly shall return to the School District all School District Data in the Company's possession and control. If return of the data is not feasible or if the School District agrees, then the Company shall destroy the data. The Company agrees to send a written certificate that the data was properly destroyed or returned. Such certificate shall be delivered within 30 days of the date of the event triggering return/destruction (e.g., within 30 days of the termination of the Agreement, within 30 days of the School District's request or notification to the Company that the data is no longer needed for the purposes of the Agreement). The Company shall destroy School District Data in a secure manner and in such a manner that it is permanently irretrievable in the normal course of business. The only exception to the requirements of this *Section 5.3* is if the Company has express written consent from a student's parent or legal guardian consenting to the maintenance of the covered information.
- 5.4 *Authorizations.* The Company agrees to secure individual School District or parent/guardian written authorizations to maintain or use the School District Data in any manner beyond the scope of or after the termination of the Agreement.
- 5.5 *Data Breach.* For purposes of this section, "data breach" means the unauthorized disclosure of data, unauthorized provision of physical or electronic means of gaining access to data that compromises the security, confidentiality, or integrity of School Student Data, or other unauthorized access, alteration, use or release of School District Data, as well as any other circumstances that could have resulted in such unauthorized disclosure, access, alteration, or use.
- 5.5.1 In the event of a data breach, the Company agrees to the following: (1) notify the School District by telephone and email within the most expedient time possible and without unreasonable delay, but no later than 24 hours after the determination that a breach has occurred; (2) at the time notification of the breach is made, provide the School District

with the name and contact information for an employee of the Company who shall serve as the Company's primary security contact; (3) assist the School District with any investigation, including interviews with Company employees and review of all relevant records; (4) provide the School District within the most expedient time possible and without unreasonable delay, and in no case later than fifteen (15) days after notification to the School District that a data breach occurred, the number of students whose covered information is involved in the breach; the date, estimated date, or estimated date range of the breach; a description of the covered information that was compromised or reasonably believed to have been compromised in the breach; and contact information for the person who parents/guardians may contact at the Company regarding the breach; and (4) assist the School District with any notification the School District deems necessary related to the security breach. The Company agrees to comply with the terms of this *Section 5.5.1* regardless of whether the misuse or unauthorized release of School District Data is the result of or constitutes a material breach of the Agreement or this Addendum.

5.5.2 The Company shall not, unless required by law, provide any notices except to the School District without prior written permission from the School District.

5.5.3 The Company shall reimburse and indemnify the School District for all costs imposed on the School District or reasonably undertaken by the School District at its discretion associated with a data breach, including but not limited to reimbursement of costs associated with notifying individuals whose information was compromised and notifying required regulatory agencies; fees paid to provide credit monitoring to impacted individuals; legal fees, audit costs, fines, and any other fees or damages reasonably undertaken by or imposed against the School District as a result of the security breach; and any other notifications, legally mandated responses, or responses reasonably undertaken by the School District in response to the breach.

6. Prohibited Uses

6.1 The Company shall not do any of the following:

6.1.1 Sell School District Data; use or share School District Data for purposes of targeted advertising, as defined in Section 85/5 of SOPPA; or use School District Data to create a personal profile of a student other than for accomplishing the purposes described in the Agreement and this Addendum and explicitly authorized in writing by the District;

6.1.2 Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of "K through 12 school purposes," as defined by SOPPA. "Amass a profile" does not include the

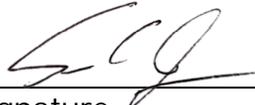
2/1/21

collection and retention of account information that remains under the control of the student, the student's parent or legal guardian, or the School District; or

- 6.1.3 Sell or rent a student's information, including covered information. This *Section* does not apply to the purchase, merger, or other type of acquisition of the Company by another entity if the Company or its successor entity complies with all relevant law and this Addendum regarding previously acquired School District Data.
- 6.2 Notwithstanding the previous paragraphs and any other terms of this Addendum, the Company may use School District Data for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application if such use is authorized by Federal or State law. The Company agrees to notify the School District if it believes release of School District Data is otherwise justified under law, including the reasons set forth in SOPPA Section 84/10(4); however, any such disclosure must be made by the School District and pursuant to valid ISSRA and FERPA exceptions.

Effective Date. The Addendum shall be deemed dated and become effective on the date the last of the parties signs as set forth below the signature of their duly authorized representatives.

Renaissance Learning, Inc.



Signature
Scott Johnson

Name
Dir. Information Security

Title
4/22/2021

Date

School District



Signature
Dave Termunde

Name
CTO

Title
6-15-2021

Date

2/1/21

Exhibit A

Agreement

N/A

2/1/21

Please refer to the attached Data Elements Collect by Product for full details.

Exhibit B
SCHOOL DISTRICT DATA PROVIDED

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>

	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>

	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student in App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>
	Other student work data-Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data-Please specify	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data-Please specify:	<input type="checkbox"/>

Other

Please list each additional data element used, stored, or collected by your application:



2/1/21

None	No Student Data collected at this time. Provider will immediately notify the District if this designation is no longer applicable.	<input type="checkbox"/>

2/1/21

Exhibit C
Nature of Products or Services Provided

The Company shall be providing the following products or services to the School District:

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; and Schoolzilla, to give educators actionable insights into trends in student attendance and achievement.

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

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

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

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

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

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

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.

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	Optional (Star CBM-US Only) *Available 5 Feb 2021*						Required	Optional	
	Testing Environment	Required (US) Optional (UK)	Required (US) Optional (UK)							
	Voice Recordings	Optional (Star CBM-US Only) *Available 5 Feb 2021*								
	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								
	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					Optional	
Schedule	Student scheduled courses	Required	Required	Required	Required				Optional	Required
	Teacher names	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

RENAISSANCE

	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			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									