Griswold Public Schools
211 Slater Ave
Griswold, CT 06351

Connecticut
Privacy Addendum to Master Subscription Agreement

This addendum ("Addendum") is hereby a part of that certain Master Subscription Agreement between Griswold Public Schools ("Subscriber") and Renaissance Learning, Inc. (Renaissance) regarding the transfer of Student Education Records to Griswold and the subsequent processing of that data. The term Subscriber includes the local or regional board of education, its school district and any one of its schools as defined below in the customer signature block. Terms not expressly defined in this Addendum shall have the same meaning assigned in the MSA. This document is effective as of the date of last signature below.

The parties agree as follows:

1. For the purposes of this Addendum, student information shall have the meaning as set forth in Public Law 16-189 and the MSA, but shall exclude directory information, de-identified information and aggregate student information ("Student Education Records"). All Student Education Records are owned by Subscriber;

2. If services are terminated by either party, and upon prior written notice by Subscriber, Renaissance agrees to delete all Student Education Records consistent with Griswold data destruction and retention policies and practices;

3. Renaissance will not use Student Education Records for any purposes other than those authorized pursuant to the MSA. Renaissance shall not use Student Education Records to engage in targeted advertising (as defined in Public Law 16-189). Renaissance shall not collect, store, or use Student Education Records or persistent unique identifiers (as defined in Public Law 16-189) for purposes other than the furtherance of Subscriber purposes. In the event Renaissance merges or is purchased by another entity, Renaissance shall notify Subscriber in writing of such merger or acquisition;

4. During the effective period of the MSA, which includes this Addendum, Subscriber shall have control of all Student Education Records provided to or accessed by Renaissance. If a parent, or guardian contacts Renaissance to review Student Education Records, and/or correct Student Education Records, Renaissance shall contact Subscriber to validate the identity of the parent or guardian and student and request instructions regarding corrective action to be taken, if any. Once validated, Renaissance shall correct erroneous Student Education Records as directed by Subscriber in writing;

5. Renaissance shall take commercially reasonable actions designed to ensure the security and confidentiality of Student Education Records.Renissance will store and process Student Education Records with commercially reasonable practices, including appropriate administrative, physical, and technical safeguards to secure such data from unauthorized access. Such measures will be no less protective than those used to secure Renaissance own data of a similar type;

6. Except as set forth in the MSA, Student Education Records shall not be retained or available to Renaissance upon completion of the contracted services unless a student, or parent or legal guardian of a student, chooses to establish or maintain an electronic account with Renaissance for sharing Student Education Records;

7. Renaissance and the Griswold board of education will ensure compliance with the federal Family Educational Rights and Privacy Act of 1974 (FERPA);

8. Renaissance will comply with applicable state personal information security breach laws when there has been a confirmed unauthorized release, disclosure, or acquisition of Student Information. In doing so, Renaissance shall maintain an incident response program that specifies the actions to be taken when Renaissance detects unauthorized acquisition or use of its information systems. As part of such response programs, Renaissance shall notify the Subscriber by email (Jcurioso@griswoldpiblicsachools.org) or telephone (860-376-7660)without unreasonable delay, but not more than thirty days, after confirmation of a breach of its security related to computer systems which contain Student Information. For the purposes of this Addendum, a breach means actual evidence of the unauthorized acquisition to or unauthorized use of Student Information ("Breach"). In the event of a Breach, Subscriber shall cooperate fully with Renaissance to ensure Griswold can comply with any notification obligations Griswold may have to the affected parent(s), legal guardian(s) or eligible student(s) or any other parties for which notification by _____ may be required under applicable law

9. Connecticut law governs the rights and duties of all parties to the MSA; and

Agreed to by:

___Renaissance Learning, Inc. _____

Printed Name	Scott Johnson
Signature	
Title	Dir. Information Security
Date	12/13/2021

Griswold Public Schools/Subscriber

Printed Name

Signature

Title

Date

RENAISSANCE

US Privacy Notice: Renaissance Products

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

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

Definitions

Capitalized words have special meaning and are defined below.

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

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

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

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

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

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

Information We Collect

We gather the various types of information below:

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

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

- 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.

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

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

Security

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

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

Data Retention and Destruction

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

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

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

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

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

Privacy Rights

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

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

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

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.

Effective Date: 5/21/2021

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

RENAISSANCE

Information Security Overview

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

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

Technical Controls

Data Storage & Hosting

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

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

Data Location

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

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

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

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

Encryption

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

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

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

Passwords and Role-Based Access

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

Network Security Features

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

Application Security Testing

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

Business Continuity & Disaster Recovery

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

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

Physical Controls

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

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

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

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

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

Administrative Controls

Risk Management Approach

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

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

Governance

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

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

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

Incident Response Team

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

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

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

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

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

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

Security Education, Training & Awareness

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

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

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

Compliance

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

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

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

RENAISSANCE

Data Elements: Collected by Product

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

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

RENAISSANCE

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

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

RENAISSANCE

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

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com

RENAISSANCE

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

©Copyright 2021 Renaissance Learning, Inc. All rights reserved. | (800) 338-4204 | www.renaissance.com