Central Islip Union Free School District
Program Information and Data Privacy Third Party Agreement

To be completed **by the vendor** and submitted for all NEW and RENEWAL software/programs prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor.

Software/Program Title:	myON
Publisher:	Renaissance Learning, Inc.
Contract Pricing	☐ BOCES Contract or Shared Service ☐ NYS or Federal Contract Pricing ☐ Direct Pricing, Bid or RFP with Vendor ☐ Free Version/Freemium
Single-Sign-On Options	☐ SSO Available through Azure AD/SAML ☑ SSO through Clever ☐ NO SSO Option ☐ N/A - Non-User Based Program/Not Applicable
License Structure:	☐ Per-User ☑ Per-Student ☑ Per-Teacher/Classroom ☑ Per-Building ☐ Districtwide/Unlimited ☐ N/A - Not Applicable or Free Version
SIS-PowerSchool Integrations	☐ Program DOES NOT sync to SIS (PowerSchool) ☐ Program DOES sync to SIS (PowerSchool) ☑ N/A - Not Applicable

ALL LINKS MUST BE PROVIDED AND COMPLETED BY THE VENDOR!

Software Title:	myON
Publisher/Developer:	Renaissance Learning, Inc.
Developer/Vendor Name:	Renaissance Learning, Inc.
Developer/Vendor Mailing Address:	2911 Peach Street, Wisconsin Rapids, WI 54494-1905
Developer/Vendor Privacy Policy Link:	https://renaissance.widen.net/view/pdf/rtvix11tcw/US-Terms-of-Service-and-License---Exhibit-D---Personal-Data-Annex.pdf?u=zceria https://www.renaissance.com/privacy/

This Data Privacy Agreement ("DPA") is by and between the Central Islip Union Free School District (herein known as "EA"), an Educational Agency, and the above listed software, app or extension developer (herein known as "Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. Breach: The confirmed unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a confirmed Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. Commercial or Marketing Purpose: means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. Disclose: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
4. Education Record: An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. Educational Agency: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. Eligible Student: A student who is eighteen years of age or older.

7. Encrypt or Encryption: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. NIST Cybersecurity Framework: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. Parent: A parent, legal guardian or person in parental relation to the student.
10. Personally Identifiable Information (PII): Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
11. Release: Shall have the same meaning as Disclose.
12. School: Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. Student: Any person attending or seeking to enroll in an Educational Agency.
14. Student Data: Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. Subcontractor: Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. Teacher or Principal APPR Data: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law: In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); to the extent applicable, Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section
2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules, and regulations.

2. Authorized Use: Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan: Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with applicable New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy: State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit: No more than once a year, or following a confirmed unauthorized access, upon ~~U~~upon receipt of a written request by the EA with at lease thirty (30) business days' notice, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, no more than once annually, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.
   (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
   (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
   (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
   (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
   (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena

in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training: Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination: The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. ~~Data Return and~~ Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond ninety (90) days following expiration or termination of the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, ~~or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA~~ or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall delete and destroy ~~transfer~~ PII~~, in a format agreed to by the Parties to the EA.~~

(b) ~~If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so,~~ Contractor agrees to ~~return or~~ destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Upon written request from EA, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition: Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption: Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any confirmed Breach of PII without unreasonable delay no later than seven
(7) business days after confirmation ~~discovery~~ of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address: Philip K. Voigt, Director of Technology at Central Islip SD, 50 Wheeler Rd, Central Islip, NY 11722.

13. Cooperation with Investigations: Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals: Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination: The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access: Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security: As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence: In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution: This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breeches or intrusions associated with this program, applications, software or browser extension.

_____ _____

Signature of Vendor Official Representative Date

If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to Philip K. Voigt, Director of Technology at Central Islip SD, 50 Wheeler Rd, Central Islip, NY 11722. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Description of the purpose(s) for which Contractor will receive/access PII	Description: Please see Renaissance's Information Security Overview for more details. ☐ NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☑ Employee PII ☐ NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE See attached Renaissance Categories of Data Collected by Assessment Period
Contract Term	Each Data Privacy Agreement is valid through the software renewal period or 1 Year for non-paid/free/pilot programs.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: ☐ Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. ☑ Securely delete and destroy data. ☐ NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written/emailed request.
Encryption	☑ Data will be encrypted while in motion and at rest. ☐ NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE

As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breeches or intrusions associated with this program, applications, software, or browser extension.

Signature of Vendor Official Representative _____ Date _____

If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.

Renaissance

See Every Student.

Categories of Data collected by Assessment Products:

Data Category	Data Elements	DnA	Fastbridge	myIGDIs	SchoolCity	StarPhonics	Star Assessment	Star Early Literacy
Application Technology Metadata	IP addresses of users; Use of cookies, etc.	Required	Required		Required	Required	Required	Required
	Other application technology metadata		Required	Required	Required	Required	Required	Required
Application Use Statistics	Metadata on user interaction with application	Required	Required	Required	Required	Required	Required	Required
Assessment	Standardized test scores	Optional			Optional		Optional	
	Observation data		Optional	Required	Optional	Optional	Optional (Star CBM-US Only)	
	Testing environment				Required		Required (US) Optional (UK)	Required (US) Optional (UK)
	Voice Recordings				Optional		Optional (Star CBM-US Only)	
	Other assessment data	Optional			Optional		Optional (Star CBM-US Only)	
Attendance	Student school (daily) attendance data	Optional						
	Student class attendance data	Optional		Optional				
Communication	Online communications that are captured (emails, blog entries)							

Data Category	Data Elements	DnA	Fastbridge	myIGDIs	SchoolCity	StarPhonics	Star Assessment	Star Early Literacy
Demographics	Conduct or behavioral data	Optional	Optional (SAEBRS & mySAEBRS)					
	Date of Birth	Required	Optional	Required	Required		Optional	Required
	Place of Birth	Optional						
	Gender	Required	Optional	Required	Optional		Optional	Optional
	Ethnicity or race	Optional	Optional	Optional	Optional		Optional	Optional
	Specialized education services (IEP or 504)	Optional	Optional	Optional	Optional		Optional	Optional
	Living situations (homeless/foster care)	Optional			Optional		Optional	Optional
	Language information (native, preferred or primary language spoken by student)	Optional	Optional	Optional	Optional		Optional	Optional
	Other indicator information	Optional			Optional			
Enrollment	Student school enrollment	Required	Required	Required	Required	Required	Required	Required
	Student grade level	Required	Required	Optional	Required	Required	Required	Required
	Homeroom			Required				
	Guidance counselor							
	Specific curriculum programs	Optional						

Data Category	Data Elements	DnA	Fastbridge	myIGDIs	SchoolCity	StarPhonics	Star Assessment	Star Early Literacy
Enrollment	Year of graduation	Optional						
	Other enrollment information	Optional						
Parent/ Guardian Information	Address	Optional						
	Email	Optional			Required (For Parent Portal)		Optional	Optional
	Phone	Optional						
	First and/or Last	Optional			Required (For Parent Portal)			
Schedule	Student scheduled courses	Required			Required		Required	Required
	Teacher names	Required		Required	Required	Required	Required	Required
	Teacher emails	Optional		Required	Required	Required	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
	Medical alerts/ health data	Optional						
	Student disability information	Optional	Optional	Optional	Optional		Optional	Optional
	Student technology needs: assistive technology & accommodations						Optional- US Only: Star Math; Star Reading; Star Reading K12	Optional

Data Category	Data Elements	DnA	Fastbridge	myIGDIs	SchoolCity	StarPhonics	Star Assessment	Star Early Literacy
Student Contact Information	Address	Optional						
	Email	Optional			Required (for SSO)			
	Phone	Optional						
Student Identifiers	Local (School district) ID number	Required	Optional	Required	Required	Required	Optional	Optional
	Vendor/App assigned student ID number		Required	Required	Required		Required	Required
	Student App username	Optional	Required		Required		Required	Required
	Student app passwords encrypted only for SSO	Optional	Required		Optional		Required	Required
	First and/or Last	Required	Required	Required	Required	Required	Required	Required
Student In App Performance	Program/ Application performance (assessment performance)	Optional	Required	Required	Required	Required	Required	Required
Student Survey Responses	Student responses to surveys or questionnaires	Optional		Required	Optional		Required	Required
Student Work	Student generated content: writing, pictures, etc.	Optional			Optional			
	Other student work data				Optional			
Transcript	Student course grades	Optional						

Data Category	Data Elements	DnA	Fastbridge	myIGDIs	SchoolCity	StarPhonics	Star Assessment	Star Early Literacy
Transcript	Student course data	Optional						
	Student course grades/ performance scores	Optional						
	Other transcript data	Optional						
Transportation	Other transportation data							

Categories of Data collected by Data & Connection Products:

Data Category	Data Elements	EduCLIMBER	eSchoolData	Schoolzilla	Schoolzilla Starter
Application Technology Metadata	IP addresses of users; Use of cookies, etc.	Required	Required	Required	Required
	Other application technology metadata	Required	Required	Required	Required
Application Use Statistics	Metadata on user interaction with application	Required	Required	Required	Required
Assessment	Standardized test scores	Optional	Optional	Optional	
	Observation data	Optional	Optional	Optional	
	Testing environment				
	Voice Recordings				
	Other assessment data	Optional	Optional	Optional	
Attendance	Student school (daily) attendance data	Optional	Required	Optional	
	Student class attendance data	Optional	Required	Optional	
Communication	Online communications that are captured (emails, blog entries)		Optional		
Demographics	Conduct or behavioral data	Optional	Required	Optional	
	Date of Birth	Required	Required	Optional	Optional
	Place of Birth		Required	Optional	

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

Data Category	Data Elements	EduCLIMBER	eSchoolData	Schoolzilla	Schoolzilla Starter
Schedule	Student scheduled courses	Required	Required	Optional	Required
	Teacher names	Required	Required	Optional	Required
	Teacher emails	Optional	Required	Optional	Required
Special Indicator	English language learner information	Optional		Optional	Optional
	Low income status- SES Free and Reduced	Optional	Required	Optional	Optional
	Medical alerts/ health data		Optional		
	Student disability information	Optional	Required	Optional	Optional
	Student technology needs: assistive technology & accommodations				
Student Contact Information	Address	Optional	Required	Optional	
	Email	Optional	Optional	Optional	
	Phone	Optional	Optional	Optional	
Student Identifiers	Local (School district) ID number	Required	Required	Required	Optional
	Vendor/App assigned student ID number	Required	Required	Required	Required
	Student App username	Required	Required	Optional	
	Student app passwords encrypted only for SSO	Required	Required		Required
	First and/or Last	Required	Required	Required	Required

Data Category	Data Elements	EduCLIMBER	eSchoolData	Schoolzilla	Schoolzilla Starter
Student In App Performance	Program/ Application performance (assessment performance)	Optional	Optional		
Student Survey Responses	Student responses to surveys or questionnaires	Optional			
Student Work	Student generated content: writing, pictures, etc.	Optional	Optional		
	Other student work data	Optional	Optional		
Transcript	Student course grades	Optional	Required	Optional	
Transcript	Student course data	Required	Required	Optional	
	Student course grades/ performance scores	Optional	Required	Optional	
	Other transcript data			Optional	
Transportation	Other transportation data	Optional	Optional		

Categories of Data collected by Practice & Instruction Products:

Data Category	Data Elements	Accelerated Reader	Accelerated Math	myON	Freckle	Lalilo
Application Technology Metadata	IP addresses of users; Use of cookies, etc.	Required	Required	Required	Required	Required
	Other application technology metadata	Required	Required	Required	Required	Required
Application Use Statistics	Metadata on user interaction with application	Required	Required	Required	Required	Required
Assessment	Standardized test scores				Optional	
	Observation data					
	Testing environment					
	Voice Recordings			Optional		Optional
	Other assessment data			Optional	Optional	
Attendance	Student school (daily) attendance data					
	Student class attendance data					
Communication	Online communications that are captured (emails, blog entries)			Optional		
Demographics	Conduct or behavioral data					
	Date of Birth	Optional (US) Required (UK)	Optional			
	Place of Birth					

Data Category	Data Elements	Accelerated Reader	Accelerated Math	myON	Freckle	Lalilo
Demographics	Gender	Optional	Optional			
	Ethnicity or race	Optional	Optional			
	Specialized education services (IEP or 504)	Optional	Optional			
	Living situations (homeless/foster care)	Optional	Optional			
	Language information (native, preferred or primary language spoken by student)	Optional	Optional		Required	Optional
	Other indicator information					
Enrollment	Student school enrollment	Required	Required	Required	Required	Required
	Student grade level	Required	Required	Required	Required	Required
	Homeroom					Required
	Guidance counselor					
	Specific curriculum programs					
Enrollment	Year of graduation					
	Other enrollment information					
Parent/ Guardian Information	Address					
	Email	Optional	Optional			Optional
	Phone					
	First and/or Last	Optional				

Data Category	Data Elements	Accelerated Reader	Accelerated Math	myON	Freckle	Lalilo
Schedule	Student scheduled courses	Required	Required			Required
	Teacher names	Required	Required	Required	Required	Required
	Teacher emails	Required	Required	Required	Required	Required
Special Indicator	English language learner information	Optional	Optional			
	Low income status- SES Free and Reduced	Optional	Optional			
	Medical alerts/ health data					
	Student disability information	Optional	Optional			
	Student technology needs: assistive technology & accommodations					
Student Contact Information	Address					
	Email					
	Phone					
Student Identifiers	Local (School district) ID number	Optional	Optional	Required	Optional	Optional
	Vendor/App assigned student ID number	Required	Required	Required		Required
	Student App username	Required	Required	Required		Required
	Student app passwords encrypted only for SSO	Required	Required	Required		Required
	First and/or Last	Required	Required	Required	Required	Required

Data Category	Data Elements	Accelerated Reader	Accelerated Math	myON	Freckle	Lalilo
Student In App Performance	Program/ Application performance (assessment performance)	Required	Required	Required	Required	Required
Student Survey Responses	Student responses to surveys or questionnaires	Required	Required	Optional	Required	
Student Work	Student generated content: writing, pictures, etc.			Optional	Optional	
	Other student work data					
Transcript	Student course grades					
Transcript	Student course data					
	Student course grades/ performance scores					
	Other transcript data					
Transportation	Other transportation data					

RENAISSANCE

Information Security Overview

Welcome educators! As a leading provider of technology products to K–12 schools worldwide, information security is a critical aspect of Renaissance's business. We abide by our regulatory obligations and strive to exceed the 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 your data. If you are interested in learning more about how we handle the privacy of your data (data use, collection, disclosure, and deletion) please visit our Privacy Hub for more information.

Technical Controls

Data Storage & Hosting

Cloud-Hosted Products:

Renaissance cloud products are designed around the core pillars of confidentiality, integrity, and availability. Renaissance products are developed, tested, and deployed in Amazon Web Services (AWS) and Google Cloud Platform (GCP) across several geographically and logically separated locations. AWS and GCP comply with an array of industry recognized standards including ISO 27001 and SOC 2.

Amazon Web Services (AWS) Hosted Products:
Renaissance Growth Platform, Freckle, myON, Schoolzilla, Star Phonics, Lalilo, EduClimber, FastBridge, eSchoolData

For more information about AWS, please visit https://aws.amazon.com/about-aws/global-infrastructure/.

Google Cloud Platform (GCP) Hosted Products:
SchoolCity, DNA, EduClimber

For more information about GCP, please visit https://cloud.google.com/infrastructure/.

Renaissance Data Center:

The Renaissance Data Center (RDC) serves our international Renaissance Place customers and is located in Wisconsin, USA. Renaissance Place runs on dedicated servers, network infrastructure, and data stores. Each customer's data is stored in a separate database that operates independently of all other customers' databases. Each school or trust that uses Renaissance Place has its own unique Renaissance hosted site URL, and each user is assigned unique login credentials.

Data Location & Vendors/Sub-Processors

See our list of Sub-Processor information.

Encryption

Data encryption is an important component of the protection of sensitive data. Renaissance's security team consistently reviews, and updates encryption controls based on the latest standards and guidelines published by Open Web Application Security Project (OWASP) and National Institute of Standards and Technology (NIST).

- *In transit:* Renaissance requires encryption over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard protocols, ciphers, algorithms, and key sizes.
- *At rest:* Renaissance requires encryption using industry standard Federal Information Processing Standards (FIPS) approved encryption algorithms.

Credentials and Role-Based Access

Each school or district has a unique identifier within 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.

Cybersecurity Features

Renaissance implements layered network security controls to protect customers' data. These include Endpoint Detection and Response software and services; next-generation firewalls; segmented design; patching; system hardening processes; and several vulnerability scanning techniques. Renaissance collects and analyzes an array of log data including system logs, system security configuration logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. We monitor systems 24 hours a day, 7 days a week and any suspicious activity is promptly investigated.

Application Security Testing

Dynamic Application Security Testing (DAST) is run against all our applications on a regular basis. The DAST process, which is an integral piece of our software development cycle, tests our software for exploitable weaknesses and vulnerabilities at each stage of the development process.

Penetration Testing

Renaissance engages with a third party to conduct penetration tests on each application and its underlying infrastructure annually. Penetration test results are used to validate all the security controls we've implemented. All penetration test findings are assessed and remediated through our change management processes and product deployment pipelines.

Business Continuity & Disaster Recovery

Renaissance maintains and tests Business Continuity and Disaster Recovery plans to protect your data. Backups are protected using segmentation and vaulting technologies. Additionally, services are deployed into scalable groups and are load balanced across compute and storage services running in geographically diverse availability zones to provide high availability and reduce 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.

Physical Controls

Cloud-Hosted Products:

Renaissance cloud products are powered by AWS and GCP: durable technology platforms that align to an array of industry-recognized standards. AWS and GCP 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/.

For more information about GCP, please visit https://cloud.google.com/infrastructure/.

Renaissance Data Center:

The Renaissance Data Center, which hosts the international Renaissance Place product, is located at Renaissance's corporate headquarters in Wisconsin. Entry into Renaissance properties is controlled via employee magnetic key entry.

Only Cloud Operations and Network Services personnel who are responsible for management of data center 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 monitor network bandwidth consumption.

The environmental conditions within the data center are maintained at a consistent temperature and humidity range, with a third-party security firm monitoring 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-start generator provides uninterrupted power to our servers and heating, ventilation, and air conditioning units. 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 and Governance

Our security processes and controls substantially follow the FIPS 200 standard and NIST Special Publication 800-53. Renaissance also assesses its Information Security and Privacy programs against the Center for Internet Security (CIS) Top 18 Controls and the NIST Cybersecurity Framework (CSF).

Cybersecurity Risk Committee: The Renaissance Cybersecurity Risk Committee is charged with identifying, tracking, and managing cybersecurity 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 is also charged with evaluating 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 vulnerabilities and risks. The Committee assesses all observed and perceived risks to develop policy, practices, and priorities to manage risk to an acceptable level.

Incident Response Team

Renaissance maintains an Incident Response Plan and has a standing Incident Response Team. The Incident Response Team performs Tabletop Exercises at least twice annually. Tabletop Exercise results are used to further refine the Incident Response Plan, policy, and risk management practices.

Renaissance collects and analyzes an array of log data including system logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. Monitoring and analysis of collected data occurs 24 hours a day, 7 days a week and any suspicious activity is promptly investigated and reported to responders.

Renaissance's employees and agents are obligated to protect all customer data. This includes reporting any suspected or known security breaches, theft, unauthorized release, or unauthorized interception of customer data. Should evidence of an information security incident arise, our Incident Response Team will initiate the response plan.

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

Security Education, Training & Awareness

All Renaissance employees are required to complete Privacy and Information Security training on an annual basis. Renaissance regularly communicates information about the current cybersecurity threat landscape to all

employees. Additionally, Renaissance conducts an anti-phishing and social engineering awareness and training program. Supplemental training events, such as International Privacy Week and Cybersecurity Awareness Month, are also major elements of the training program.

Compliance

Audits: Renaissance's enterprise Information Security & Compliance Program successfully completed the SOC 2 Type 1 examination of controls in November 2022. The examination is formally known as a Type 1 Independent Service Auditor's Report on Controls Relevant to Security, and reports on Renaissance's systems and the suitability of the design of our controls. Our SOC 2 Type 1 is scoped to specific products and services. For more information on our SOC audits, including which products have completed SOC audits, please contact infosecurity@renaissance.com.

Renaissance's enterprise Information Security & Compliance Program intends to complete a SOC 2 Type 2 examination of controls in 2023 and annually thereafter.

Employees: All Renaissance employees must sign a nondisclosure agreement prior to the start of their employment. Additionally, all employees are required to read, sign, and agree to abide by Renaissance's Information Security and Information Technology policies. Background checks are conducted as part of the onboarding process for employees to the extent permitted by law.

Vendors/Sub-processors that Support Our Products: Renaissance maintains a vendor compliance program. Vendors' security and privacy practices are reviewed and analyzed. Additionally, Renaissance enters into written contracts with each vendor/sub-processor containing terms that offer similar levels of data protection obligations and protection for customer personally identifiable information as identified in our Data Protection Addendum with customers.

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