This Agreement ("Agreement") is entered into by and between The Education Cooperative (hereinafter referred to as "Cooperative") and Renaissance Learning, Inc. (hereinafter referred to as "Provider") on June 11, 2018.

RECITALS

WHEREAS, the Cooperative assists school districts in Massachusetts with negotiating with providers on privacy terms; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the Cooperative to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of the Massachusetts Student Data Privacy Agreement ("DPA") in "Exhibit 1" for the Services described, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

TERMS

I.   The Provider will sign the attached DPA in "Exhibit 1", accepting its terms, without the school district being identified.

II.   The Provider agrees to offer the privacy protections found in the DPA in "Exhibit 1" to any school district in the boundaries of Massachusetts who accepts the DPA though its signature, in conformance with the laws of Massachusetts. The Provider's offer shall extend only to privacy protections and the Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in the DPA.

III.   The Cooperative can offer the DPA, signed by the Provider, to any school district in Massachusetts. After the Provider has signed, the Cooperative can add the information required in Exhibit "E" to "Exhibit 1". The Cooperative cannot make any other changes to the DPA after the Provider has signed.

IV.   The Cooperative will transmit a fully executed copy of each DPA to the Provider within ten (10) days of execution.

V.   The Provider may withdraw its offer to school districts in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in Article I and Exhibit "A" of the DPA; or (3) three (3) years after the date of Provider's signature to this Form. Provider shall notify the Cooperative in writing in the event of any withdrawal.

VI.   The parties understand and agree that they have the right to execute this Agreement and Provider has a right to execute the DPA, through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding.   They agree not to

object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request in writing to the other representative that signed below that their electronic signature be revoked if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

VII. This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

RENAISSANCE LEARNING, INC.

BY: _____   Date: _8/30/2018_____

Printed Name: _Jeff Christensen_____   Title/Position:_Director of Information Security

THE EDUCATION COOPERATIVE

BY: _____   Date:_____

Printed Name: Elizabeth McGonagle_____   Title/Position: Executive Director_____

EXHIBIT 1

MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT
VERSION (2018)

LOCAL SCHOOL DISTRICT, DEFINED IN EXHIBIT "E"

and

RENAISSANCE LEARNING, INC.

DATE, DEFINED IN EXHIBIT "E"

This Massachusetts Student Data Privacy Agreement ("DPA") is entered into by and between the school district, referenced in Exhibit "E", (hereinafter referred to as "LEA") and Renaissance Learning, Inc. (hereinafter referred to as "Provider") on the date listed in Exhibit "E". The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq.; and

WHEREAS, the documents and data transferred from Massachusetts LEAs and created by the Provider's Services are also subject to several Massachusetts student privacy laws, including Massachusetts student record regulations, 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described in Exhibit "A".

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit "B".

4. **DPA Definitions**. The definition of terms used in this DPA is found in <u>Exhibit "C"</u>. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

4. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell

2

the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

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

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

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

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all Massachusetts and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, , 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

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

4. **No Disclosure**. De-identified information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider and LEA agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.

5. **Disposition of Data**. Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within three (3) calendar days of receipt of said request.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

   b. **Destruction of Data**. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

   c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

   d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

   e. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.

   f. **Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the DPA.

   g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

5

h. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

i. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

j. **Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide full access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider. Failure to cooperate shall be deemed a material breach of the Agreement.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within ten (10) days of the incident. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

   i. The name and contact information of the reporting LEA subject to this section.

   ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

   iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

   iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

   v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

> **i.** Information about what the agency has done to protect individuals whose information has been breached.
>
> **ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in the Massachusetts Data Breach law and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

   The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be

in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this Agreement is:

Name	N/A
Title	Contract Administrator
Address	2911 Peach Street, PO Box 8036, Wisconsin Rapids, WI 54495-8036
Telephone Number	800-338-4204 / contracts@renaissance.com

The designated representative for the LEA for this Agreement is in Exhibit "E".

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MASSACHUSETTS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY LISTED IN EXHIBIT "E" FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained

therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

10. **<u>Waiver</u>**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **<u>Electronic Signature:</u>** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding.   They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. **<u>Multiple Counterparts:</u>** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

[*Signature Page Follows*]

1074647v1

IN WITNESS WHEREOF, the parties have executed this Massachusetts Student Data Privacy

Agreement as of the last day noted below.

LEA

By: _Eric DeHays_
Eric DeHays (Dec 9, 2019)

Date: 12/9/2019

Printed Name: Eric DeHays

Title/Position: Technology Director

RENAISSANCE LEARNING, INC.

By: _____

Date: 8/30/2018

Printed Name: Jeff Christensen

Title/Position: Director of Information Security

10

EXHIBIT "A"

DESCRIPTION OF SERVICES

https://www.renaissance.com/

Student assessment online application

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	X

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts	X
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	X

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	

12

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	X

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of "school official" encompasses the definition of "authorized school personnel" under 603 CMR 23.02.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

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

Third Party: The term "Third Party" means an entity that is not the provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

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

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable

_____ By (Insert Date]

4. Signature

_____
(Authorized Representative of LEA

_____
Date

5. Verification of Disposition of Data

_____   _____
Authorized Representative of Company   Date

REQUIRED INFORMATION

SCHOOL DISTRICT NAME: Ashburnham Westminster Regional School District
_____

DATE: 12/9/2019
_____

DESIGNATED REPRESENTATIVE OF LEA:

Name   Eric DeHays
_____

Title   Technology Director
_____

Address   11 Oakmont Drive, Ashburnham MA, 01430
_____

Telephone Number   978-827-1434
_____

COUNTY OF LEA: _____

DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1.   Does your organization have a data security policy? ☒ Yes   ☐ No

        If yes, please provide it. Please see attached

2.   Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

        ____ ISO 27001/27002

        ____ CIS Critical Security Controls

        _X_ NIST Framework for Improving Critical Infrastructure Security

        ____ Other: _____

3.   Does your organization store any customer data outside the United States? ☐ Yes ☒ No

4.   Does your organization encrypt customer data both in transit and at rest? ☒ Yes   ☐ No

5.   Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

        Name: Jeff Christensen, Director of Information Security

        Contact information: Jeff.Christensen@renaissance.com; 800-338-4204

6.   Please provide any additional information that you desire.

Renaissance data privacy and security plan

Data center infrastructure and security procedures

Renaissance stores all data within the United States, inside secure data centers. Our primary data center is located in Wisconsin Rapids, Wisconsin; for security reasons, we do not publicly disclose the locations of our backup data center sites.

Entry into Renaissance's corporate headquarters, which houses the data center, is controlled via employee magnetic key entry. Access to the data center is strictly limited. Only the hosting services department and information system employees who are responsible for the entire corporate infrastructure are allowed unescorted access to the Renaissance Place data center. Access 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 maintain a high level of security and prevent unauthorized access to customer data by monitoring log files, reviewing access logs, tracking system usage, and monitoring network bandwidth consumption.

Renaissance takes appropriate steps to safeguard the integrity of our customers' data. Each customer's data is stored in a separate directory and database that operates independently of every other customer's directory and database. This allows us to keep customer data separate and secure while minimizing system resources. We monitor all hosted servers 24 hours a day, 7 days a week, using various physical and automated methods.

Standards compliance

Renaissance takes security seriously. Below is a list of key standards, laws, and guidelines that we follow:

- Our security structures and controls substantially follow the National Institute of Standards and Technology's Federal Information Processing Standards (FIPS) 200 standard and related FIPS publication 800-53.

- We follow the IT Internal Governance Institute's guidelines on internal governance and operations of our systems.

- We follow the payment card industry (PCI) standards for processing credit card information.

- We are compliant with FERPA requirements.

- Our application software is independently reviewed annually against the Open Web Application Security Project programming guidelines. In addition, penetration and vulnerability assessments are regularly conducted by third-party system security firms.

- Renaissance has signed the Student Data Privacy Pledge created by advocacy groups and endorsed by the White House. For more information regarding this pledge visit http://studentprivacypledge.org.

Physical and network security procedures

Renaissance takes appropriate steps to safeguard the integrity of our customers' data. Each customers' data is stored in a separate directory and database that operates independently of every other customer's directory and database. This allows us to keep customer data separate and secure while minimizing system resources. We monitor all hosted servers 24 hours a day, 7 days a week, using various physical and automated methods, which we describe below. Any suspicious activity is promptly investigated and addressed. In addition, we do not disclose any student or teacher information from customer databases to any third party without prior written consent.

Disaster recovery

Our data center's physical security systems ensure that equipment remains functional and customer data protected in the case of any emergency, such as a power outage or natural disaster. If a power outage occurs, an automatic generator provides uninterrupted power to our servers and HVAC units. A waterless Inergen fire protection system and an early warning water detection system help us to prevent any damage to the servers that store your data in the case of an unforeseen calamity.

Renaissance maintains a geographically separate warm backup site for disaster recovery of our services. Below we provide our backup retention periods:

- Full backups: Two nights a week

- Differential backups: Five nights a week (the nights when full backups do not occur)

- Transaction log backups: 24 hours a day, 7 days a week, every 20 minutes

Full and differential backups are transmitted nightly to a secure Renaissance facility not housing the data center. Backups are also transmitted nightly to our disaster recovery site.

Monthly archives are stored in a secure location offsite and held for three months.

Physical security

Renaissance strictly monitors access to the data center. Unescorted access to the Renaissance Place data center is limited to the Renaissance hosting services department and information system employees who are responsible for the entire corporate infrastructure. Entry into Renaissance's corporate headquarters, which houses the data center, is controlled via employee magnetic key entry. Entry into the Renaissance Place data center itself is controlled through a proximity card access system and a motion-based detection system so that only data center and networking personnel may enter. All visitors to the data centers, as well as their internal employee escorts, must sign an access log. To maintain a high level of security and prevent authorized access to customer data, we review access logs on a regular basis.

Network security

Renaissance protects customers' data from electronic intrusion by practicing vigorous network security procedures. Processes are in place to monitor log files and check for unauthorized access. Renaissance has monitoring and tracking methods for system usage and network bandwidth consumption in place. Upon any evidence of intrusion or unauthorized access, a formal counter measure process is executed that includes, but is not limited to, the following

- Severing the connection of the intruder to the compromised system(s), including but not limited to restricting IPs in Internet Information Services, disabling services, and powering off the Renaissance Place virtual server

- Notifying the affected data owners

- Notifying the Renaissance department directors and executives

- Assessing the damage from the intrusion

- Assessing the intrusion and correcting security vulnerabilities

- Reporting assessment, damage, and remedies to the data owner

Renaissance implements the following network security measures to protect customers' data:

- Transport Layer Security (TLS) using 2048-bit third-party certificates that provide 256-bit encryption

    - TLS provides confidentiality and integrity of all data transmission over untrusted networks to Renaissance products. Renaissance uses the same TLS communications that are widely trusted by leading financial institutions for electronic commerce and online transactions. By default, each of our client applications also

connect using TLS. Using industry standard 256-bit encryption ensures that customer data traversing the Internet cannot be intercepted and read by eavesdroppers.

- Multiple firewalls

    – The servers located within our internal network are behind stateful firewalls as well as Web Application Firewalls (WAFs). Data travels between our web servers and database servers through specific white-listed data ports. Renaissance forces HTTPS over TLS on port 443 for all Renaissance Place application communication. Firewalls allow only these ports carrying your data to be open to the web servers. In doing so, firewalls prevent improper content from entering the internal network, reaching the database servers where your data is stored, and threatening the confidentiality, integrity and availability of your data.

- Antivirus (AV) software, Intrusion Prevention System (IPS), and Operating System (OS) updates

    – AV software is installed on all hosted servers to protect against computer malware. We perform regularly scheduled full system scans and update AV definitions per manufacturer's specifications.

    – IPS monitors and protects egress points at the network perimeter.

    – Operating Systems are regularly patched and critical updates are expedited as necessary. For added security, we test all update patches on non-production QA hosted systems prior to releasing them into production hosted systems. These patches mitigate security vulnerabilities and software bugs that may interfere with optimal functionality and reliability of the hosted server environment.

Data security training

In accordance with Renaissance's data security and privacy Plan, Renaissance agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of Renaissance who will have access to the shared student data, have received or will receive annual training on the federal and state law governing confidentiality of such data prior to receiving the data or access to the data. Upon request, Renaissance and/or its subcontractors or assignees will provide a certification from an appropriate officer that the requirements of this paragraph have been satisfied in full.

Encryption technology

Renaissance uses industry-standard encryption technology to protect all access to data while in transit. Tables containing passwords are also encrypted at rest.

Access control to only those with educational interests

Renaissance follows industry-standard procedures to maintain optimal security once customers are ready to create user accounts in Renaissance Place. These procedures include defining user permissions based upon individuals' roles within the school district, authenticating users to guarantee that only authorized individuals gain access to the system, and encouraging users to follow recommended password security protocols.

User permissions and authentication

Renaissance's product software contains seven defined user groups, including district administrator, district staff, school administrator, school staff, teachers, parents, and students. The system administrator assigns each user to one of these user groups and to a specific position within that group. Each user is then assigned capabilities, which gives them the right to perform specific, pre-assigned tasks in the software based on their user group and the tasks that the user group usually performs. These settings also allow different levels of access to the software's administrative features and to data. For example, district administrators have access to reports for all levels—individual students, classes, teachers, schools, and the district as a whole—while teachers can view reports only for their students and classes. Some staff members, however, may perform more than one role in the school or district, or they may be assigned to more than one school. The system keeps track of these multiple roles and school assignments and allows these users to switch between roles or schools while they are using the software.

Authentication of users is self-contained within the Renaissance Place system. To authenticate users, Renaissance Place uses the forms authentication model included in Microsoft's ASP.NET framework. Within this model, a user logs

in to Renaissance Place and enters his or her password, which is validated against the encoded password associated with that user and stored in the system database. Lightweight Directory Access Protocol (LDAP) authentication against Windows Active Directory is provided as an optional part of our data integration service (RDI).

Password security

To access programs in Renaissance Place, all users—including administrators, teachers, parents, and students—must enter a user name and password. These user names and passwords can be any combination of alphabetical, numeric, or symbol characters. When a system administrator creates user accounts in the system, users are automatically assigned a temporary password. The first time users log in with their temporary passwords, the system requires them to change their passwords. Note that the system does not enforce strong passwords. Instead, customers are responsible for managing the access rights of their employees and students and the enforcement of their internal password and access rights policies and internal practices regarding privacy.

If users forget their passwords or receive a message that their password has expired (this occurs every 365 days), they can reset it by following the Forgot Your User Name or Password? link on the login screen. The system will ask them for their user name and then allow them to reset their password by either (1) entering a valid e-mail address, or (2) providing the correct answer to one of three pre-set security questions. For this feature to function, users will first need to provide and validate their e-mail address. To ensure this is done in advance, the system automatically prompts users to establish these settings the first time they log in to Renaissance Place.

Additionally, if users try unsuccessfully to log in three times, they will be locked out of the system. This lock will automatically be released every evening at midnight. To unlock the account more quickly, users can use the reset procedure described above.

Users should change their passwords periodically as a safeguard against unauthorized access to their account. While Renaissance Place requires that users update their passwords annually, they may manually update their passwords more frequently. System administrators can also force the system to prompt password changes.

Data disclosure (Statement of Use)

Renaissance has implemented practices and policies to ensure that the products and services we provide protect confidential information. Information considered confidential includes student records, teacher and administrative contact information, school and district profiles, and any other customer data housed in our products or databases. All of our employees have a responsibility to protect this data and to take all necessary precautions to assure that it is never released unless authorized.

No data is collected by third parties. Renaissance will not disclose any student or teacher information from customer databases to any third party without prior written consent.

Further, we comply with and follow these key security and confidentiality standards, laws and guidelines:

- Applicable requirements of the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy and Protection Act (COPPA), the Children's Internet Protection Act (CIPA, CIPA-2), and the Health Insurance Portability and Accountability Act (HIPAA).
- The Student Data Privacy Pledge (http://studentprivacypledge.org), which Renaissance has signed. The legally binding commitments in the Pledge can be enforced by the Federal Trade Commission and states' Attorneys General.
- The National Institute of Standards and Technology's Federal Information Processing Standards (FIPS) 200 standard and related FIPS publication 800-53 for security structures and controls.
- The IT Internal Governance Institute's guidelines on internal governance and operations of our systems.
- The payment card industry (PCI) standards for processing credit card information.

Only Renaissance employees who have direct responsibility to support customers' operation of Renaissance Place have access to customer and student information. We maintain a Security Committee, which has a mandate to adopt, implement, and audit policies and controls that ensure effective security practices. To ensure a high level of visibility, this committee reports directly to our senior executive management.

Data return or destruction upon contract end or termination

Any data collected by Renaissance products used by customers is the sole property of customers at all times, during and/or after the expiration of this contract. Renaissance Learning, Inc., possesses the legal ownership, right and title to any data, materials or intellectual property inventions or discoveries made or conceived by Renaissance prior to or during, or in connection with this contract and to use anonymous, non- personally identifiable data collected by Renaissance products: (i) to maintain and improve application performance or functionality (ii) for general research and, (iii) for other valid purposes.

Renaissance will delete student records only when requested in writing by the school district, when required to by law or court order, or after the customer terminates its subscription. This does not prohibit the retention of archival back-ups and the retention of performance data that is not identifiable to a specific student, classroom, school, or district.

If a customer elects not to renew its contract with Renaissance, the data will be purged 90 days after the contract's end date, when we destroy the final back-up files.

Ability to challenge data accuracy

Renaissance is compliant with FERPA requirements. In the event that a parent or eligible student wishes to challenge the accuracy of the shared data concerning that student or eligible student that is maintained by Renaissance, that challenge may be processed through procedures provided by the licensed component district for amendment of education records under FERPA.

In addition, our student assessment products all require users to sign on using their individual user name and password. Student assessment activity is recorded in the Renaissance Place database, and numerous reports within Renaissance Place allow teachers and administrator to review this activity. User activity involving the creation or modification or data (tracking the number of students taking test, creating and inputting new class data, and updating student enrollment numbers) is recorded in the database and available to appropriate Renaissance technical personnel as needed.

Subcontractor security protocols

In accordance with FERPA, Renaissance shall not disclose any personally identifiable student records from the hosted application's database to any third party except: (i) if required by law or valid court order, (ii) as directed in writing by the customer or, (iii) as permitted elsewhere in the Renaissance Application Hosting Agreement. Renaissance and its contractors may use data in the hosted application's database: (i) to maintain and improve application performance or functionality, (ii) for general research and, (iii) for other valid purposes. Any contractors of Renaissance shall be subject to the same obligation of confidentiality as Renaissance.

The customer will not disclose to any third party any confidential or proprietary information of Renaissance or any technical information relative to the setup and security of the hosting service, including but not limited to hosting service Internet addresses, passwords, Internet URL's, Virtual Private Network setup, and encryption key information, unless such disclosure is approved in writing by Renaissance.

RenaissanceDPA_TEC-signed083118 (2)

Final Audit Report   2019-12-09

Created:	2019-12-08
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA92oH0LM11DEyqdWMA0giRltEGVCv92G2

"RenaissanceDPA_TEC-signed083118 (2)" History

📄 Document created by Ramah Hawley (rhawley@tec-coop.org)
2019-12-08 - 12:39:44 PM GMT- IP address: 100.1.115.187

✉ Document emailed to Eric DeHays (edehays@awrsd.org) for signature
2019-12-08 - 12:41:18 PM GMT

📄 Email viewed by Eric DeHays (edehays@awrsd.org)
2019-12-09 - 1:20:23 PM GMT- IP address: 66.102.8.63

✍ Document e-signed by Eric DeHays (edehays@awrsd.org)
Signature Date: 2019-12-09 - 1:22:09 PM GMT - Time Source: server- IP address: 40.138.23.82

✅ Signed document emailed to Ramah Hawley (rhawley@tec-coop.org) and Eric DeHays (edehays@awrsd.org)
2019-12-09 - 1:22:09 PM GMT