Standard Student Data Privacy Agreement

IL-NDPA v1.0a

School District or LEA

Crete-Monee School District 201-U

and

Provider

Renaissance Learning, Inc.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

[Crete-Monee School District 201-U], located at [1515 West Exchange St., Crete. IL 60417] (the "**Local Education Agency**" or "**LEA**") and

[Renaissance Learning, Inc.], located at [2911 Peach St., Wisconsin Rapids WI 54494] (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   ☑ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**

   ☐ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: _____Title: _____

Address: _____

Phone: _____Email: _____

The designated representative for the Provider for this DPA is:

Name: Stephanie Carver Title: Corporate Counsel & Data Protection Officer

Address: 6625 W 78th Street, Suite 220, Bloomington, MN 55439

Phone: (800) 338-4204 Email: privacy@renaissance.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Crete-Monee School District 201-U

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

Provider: Renaissance Learning, Inc.

By: _____ Date: 04/26/2021

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

STANDARD CLAUSES
Version 1.0

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

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

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

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

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

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees 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. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
Lalilo by Renaissance is hosted in Amazon Web Services in France. In order to better serve our US customers, Lalilo by Renaissance anticipates adding a US-based Amazon Web Services region dedicated to our US customers within 2021.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable 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 LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

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

(2) Provider agrees to adhere to all federal and state requirements 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.

(3) 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 summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute 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.

5. **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.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, 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.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

As a global leader in assessment, reading, and math solutions for pre-K–12 schools and districts, Renaissance is committed to providing educators with insights and resources to accelerate growth and help all students build a strong foundation for success. Renaissance solutions are used in over one-third of US schools and in more than 90 countries worldwide.

Lalilo is an online research-based phonics and comprehension program for K-2 students and teachers.

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.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	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	

Category of Data	Elements	Check if Used by Your System
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	X
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
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	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	

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	☐
	Student bus card ID number	☐
	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application: Please refer to the attached Privacy Notice for additional information.	☐
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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 Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

Subprocessor: For the purposes of this DPA, 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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

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:

[ ]

_☑_ 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:

[ ]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_☑_ As soon as commercially practicable.

_☐_ By [ ]

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Crete-Monee School District 201-U ("Originating LEA") which is dated 4/26/2021, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: contracts@renaissance.com.

PROVIDER: Renaissance Learning, Inc.

BY: _____ Date: 04/26/2021

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

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Crete-Monee School District 201-U and Renaissance Learning, Inc.

**PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA:

BY:_____ Date:_____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☑	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G" - Supplemental SDPC (Student Data Privacy Consortium) State Terms for Illinois

Version IL-NDPAv1.0a (Revised March 15, 2021)

This **Exhibit G,** Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between Crete-Monee School District 201-U (the "Local Education Agency" or "LEA") and Renaissance Learning, Inc. (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C,** Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or

copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. **Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

8. **Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA and this Exhibit G, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. **Security Breach Notification.** In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

b. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

10. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

11. **Transfer or Deletion of Student Data.** The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

12. **Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this Exhibit G.

13. **Subcontractors.** By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

14. **DPA Term.**

a. **Original DPA.** Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."

b. **General Offer DPA.** The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: "The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."

15. **Termination.** Paragraph 1 of Article VII shall be deleted, and the following shall be inserted in lieu thereof: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.'

16. **Privacy Policy.** The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

17. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

18. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

19. **Data Storage.** ~~Provider shall store all Student Data shared under the DPA within the United States.~~
Lalilo by Renaissance is hosted in Amazon Web Services in France. In order to better serve our US customers, Lalilo by Renaissance anticipates adding a US-based Amazon Web Services region dedicated to our US customers within 2021.
20. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

EXHIBIT "H"

Additional Terms or Modifications

Version _____

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

None

Your personal data at Lalilo

- Regarding data collection, we only collect the information a teacher provides when signing up, as well as the students' learning data. We can also collect audio recordings, with the teacher's consent, during specific exercises.
- Data is only collected if we believe that this data allows us to help students in their learning and teachers in their job.
- We are committed to full transparency regarding the collection and use of school, student and teacher data.
- Teachers are held responsible for accepting this privacy policy on behalf of under-age students. They have the obligation to communicate this policy to parents or guardians of students.
- Retained data will never be used or sold for non-educational commercial or marketing purposes.

Lalilo complies with FERPA, COPPA, Ed. Law 2-D, and most privacy regulations. Our *Data Security and Privacy Plan* is available upon request to any Educational Agency willing to contract with Lalilo. This plan includes our response plan in case of a data breach.

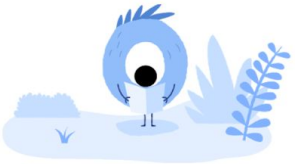
Information to reviewers

In case of a breach, Lalilo would inform users within 48 hours after discovery.

Lalilo supports or will support login through Google Classroom, Clever and other Educational SSO. Lalilo does not support login through social media accounts for students or teachers.

Lalilo does not use user-generated content, whether from students or teachers. There's no social interaction between two users, whether teachers or students.

Lalilo does not display traditional nor contextual advertisements.



Lalilo Inc.
400 Montgomery Street, Suite 1100, San Francisco, CA
privacy@lalilo.com / www.lalilo.com

What is Lalilo?

Lalilo is a teaching tool for primary school teachers. Teachers sign up on the teacher interface by entering their personal information. They can then, from the teacher's dashboard, fill in their student's ID tags on the platform.

Students can log on to their individual student interface, using a 6-letter code specific to the school in which the teacher enrolled. They then have access to a set of exercises, lessons and rewards that allow them to learn how to read at their own pace.
Students can sign in directly to their accounts from home, with an individual code that the teacher can send to parents, if they so wish.

Which data?

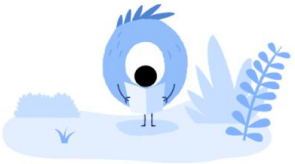
The data collected by Lalilo includes two types: 1) the data provided by the teacher when signing up and adding students, and 2) the data automatically collected by Lalilo. At no time do we ask nor will we ever ask a child to complete a form requesting personal information.

Lalilo also uses third-party applications to provide its services. They include the user support chat, our emailing tools, feedback software... The list of these third-party applications that process personal data or which can use cookies on your computer is available in the appendix.

What are my rights ? What commitments do you make?

<u>Principle of economy</u>
Generally speaking, we only collect data that is necessary for:

- the use of our product;
- the design of our product;
- the understanding of our users (teachers, children, parents).



Lalilo Inc.
400 Montgomery Street, Suite 1100, San Francisco, CA
privacy@lalilo.com / www.lalilo.com

One can learn about the details of the data and the treatments carried out on these data by Lalilo in appendix.

Principle of information and transparency

We are committed to being as thorough and clear as possible about our data collection and processing. This document will evolve, in its form and in its substance, as our users will ask us for more details about the way we process their data, and also as the features offered by Lalilo evolve.

You will be notified of all changes to the privacy policy by email to the address you provided when signing up on the platform.

We will gladly answer any questions you may have on the data collected, services used, or processing performed. Do not hesitate to contact dpo@lalilo.com for any questions regarding these topics. As we answer these questions, we will create a FAQ about our privacy policy, complementary to this document.

Our Data Protection Officer is Laurent Jolie.

Access, portability and deletion of data

As a teacher, you can:

- recover the personal data of your students or yours;
- remove the personal data of your students or yours;
- Stop the collection of personal data of your students or yours.
- Send us an email to dpo@lalilo.com from your registration email on the platform. A request from another email address will automatically be refused for obvious reasons of data security.

As a teacher, it is your responsibility to send us any request from a parent concerning the personal data of their child. In case of withdrawal of consent from a legal guardian, it is your responsibility to make sure that their child is no longer using Lalilo.

As the legal guardian of a child you can:

- recover the personal data of your child;

- have your child's personal data deleted
- stop the collection of your child's personal data.

Since you are not directly identified, the teacher will act as an intermediary for your request. You will have to ask them to make this request from the email address they used to sign up onto the platform. We reserve the right to decline any request that we consider unreasonable access to data. Some data is completely anonymized after a given time, and are no longer recoverable.

Benefit-risk balance principle

Before taking the decision to collect a new type of data, or to carry out a new treatment, we will study the benefit-risk balance of this new collection or treatment.

Speech and Audio Recordings Database

We apply a “data protection by default” and “data protection by design” approach in keeping with the principle of minimizing the processing of personal data to the extent necessary to provide the services and to further develop and enhance the voice recognition system.
We promise never to sell our database of audio recordings. This database will only be used as part of the services operated by Lalilo. This database is regularly anonymised. We will not take any step to re-identify or de-anonymize any end user voice data, and shall not authorize, instruct or encourage any third party to do so. See above the list of treatments, in the section "Audio recordings" and "Audio data processing".

Safety

We give great importance to the data security of students, teachers and potential third-party users (parents), and we set standards for safety practice. All access points to our stored data are secure, and we reduce access to data only to people who need that access. All our communications between your terminal and our server are encrypted with standard cryptographic algorithms.

Location

Our databases are physically located in France, to comply with current European regulations (RGPD).

What are my duties as a user?

Positive consent to registration
As a teacher, when signing up onto platform, you will need to provide your explicit and positive consent to this privacy policy to access the service.

Default Consent if Use Without a Change Warning Reply
We will notify you by email of changes to the privacy policy, on the email address you provided when signing up. Two choices will be offered: either to accept or to refuse. The rejection will result in the deletion of your account and all related data, including the ones of your students, within two weeks. You will no longer be able to use our platform.
If you do not respond to the change warning email or alert in the platform, and continue to use the Lalilo service, we will consider this as consent.

Consent of Students
As the vast majority of students are minors below the legal limit of consent, parental consent may be required. The responsibility for obtaining parental consent for the use of Lalilo is left to the care of the teacher and the school.

By signing this privacy policy, you agree to be fully entitled to have your students use Lalilo.

In the case of a child of which you are responsible, who is over the legal limit of your country's consent, you will need to make sure that they consent.

Applicability Framework

We disclaim any liability for any use of our platform which does not comply with our terms of use or our privacy policy. Signing up on the platform is reserved exclusively for teachers, homeschooling officers and educational leaders in specialized institutions.

Registration on the platform is PROHIBITED to parents.
The use of the platform by parents is accepted when the access code dedicated to home usage has been communicated by the student's teacher.

No other operator than Lalilo handles children's data. The data is not sold or rented to any third party, including for marketing or advertising purposes.

Lalilo is based in Paris at 96b Boulevard Raspail.
Lalilo is also based in San Francisco, CA 94111, Suite 1100 400 Montgomery Street.

For any question, remark, request for clarification or suggestion on your data, please contact dpo@lalilo.com.

Annex 1: Data processed by Lalilo

What data is communicated by the user?

Name, Surname, Email of the teacher
This information allows us to contact you, to send you information about product developments, events set up within the Lalilo teacher community and any other type of communication.

Name of your school

1. This information allows us to bring together teachers from the same school; digital terminals are often shared across the school (mobile classroom, computer room)

2. We can better know our users and improve the quality of our support (more effectively unblock situations related to districts or boards)

Teaching Language
Language in which the students will learn how to read on Lalilo

Level - Class
1. This is the only information we have on the initial level of children: this allows us to adapt the level of exercises we offer more quickly.

Students' ID tags
The ID tag is the only data communicated on students. We need it so that students can choose their own account when they log in. The choice of the ID tag is left for the teachers to choose:
- first name
- first name + last name
- initials
- other type of ID tags (superheroes, animals ...).

Data collected automatically

Learning data

When students learn how to read at their own pace on Lalilo, they interact with the platform. A number of actions are recorded by Lalilo:

- answer given or composed by the student;
- response time;
- repetition of instruction or phonemes;
- other data related solely to the assessment of student success in an exercise or understanding of a learning sequence.

This data is recorded in its raw format (a list of interaction events with the platform).
This data is kept pseudo-anonymized. Pseudo-anonymization means that learning data is

not stored in the same place as personal data. A common identifier, however, allows to link them.
The student data is anonymized after one year of inactivity.
Anonymizing these data means that we are unable to tell which student did what action.
They cease to be personal data.

Usage and Processing of learning data

Data is collected in order to be able to adapt questions in a relevant and individual way at the level of each student. Lalilo assesses the level of students on a number of skills related to literacy, using a statistical model called "IRT" (for Item Response Theory), used by statisticians in psychology.

This paradigm allows, from the raw data of learning, to calculate the prior probability of success of a student to an exercise. From this set of probabilities of success and pedagogical rules, the algorithm determines as a student progresses which are the most relevant exercises for him or her at a given moment.The educational constraints, determined with experts in education science, make it possible to provide a path of high educational quality.

The calculation times being non-negligible, and because teachers need information displayed in their teacher's dashboard, the intermediate success rates of students on various skills are stored in a pseudo-anonymized way in a table. This data is updated regularly (at each child's exercise), and will be totally deleted when the raw data is pseudo-anonymized (see section Learning Data).

Audio recordings

Lalilo integrates playback feedback and playback tracking features. The student can, in the first case, read a sentence to the machine, which corrects it and identifies mistakes. In the second case, the child can read a sentence or a longer text, and the machine is able to follow where the student is reading this sentence or longer text. Feedback can then be given to the student, so that they become aware of pronunciation and personal difficulties. Other reading exercises allowed in autonomy may be developed by Lalilo in the future.

In order to offer these features, Lalilo can retrieve on its servers the audio recorded

by the device's microphone at certain times during the session. These records are of two types:

1. Records of "background noise" in the range of a few seconds. These recordings can be made before starting a read-aloud exercise using the microphone. These are analyzed in order to estimate the relevance of giving this type of exercise. Indeed, if the background noise is too important or the equipment is working badly, it is often better not to do exercises using voice recognition. These recordings are not subject to speech recognition analysis, and a fortiori are not subject to semantic analysis. These "background noise" recordings can be randomly stored. They are stored only for the purpose of forming acoustic background noise models, making it possible to improve the pre-processing algorithms. These recordings are completely anonymous.
2. "Exercise" recordings, which are intended to specifically record the child's reading, as part of an exercise on the platform. These records are stored in our databases, in a pseudo-anonymized way for a limited period of time, so the teacher would be able to listen back to it. After this period, the recording is anonymized before being stored in the database.An annual process of total anonymisation is carried out. With each exercise, recordings are stored according to the student's country & city. This allows us to improve our acoustic models, differentiating them according to the peculiarities of the regional accents.

Processing of audio data

Lalilo's algorithms are not strictly speaking speech recognition algorithms. The purpose of the treatment is not to find which text is pronounced (in fact no semantic analysis is made on the recordings). Lalilo has created a reading evaluation algorithm. Its purpose is to detect the quality of the reading, the mistakes made and to give relevant feedback to students, in order to allow them progress.

Several treatments are done. A pre-processing is used to evaluate whether the recording is exploitable or not (see paragraph "Audio recordings"). If the recording is exploitable, the algorithm will analyze it. It will detect whether the students are hesitating as well as their pronunciation errors. From this analysis, the algorithm will determine the most relevant feedback to give students.

The result of this algorithm is recorded in the raw learning traces of students mentioned above (see section on learning data) and these are used to estimate the students' probability of success (see Treatment section on learning data).

Lalilo uses for some exercises a tracking algorithm. This algorithm allows to follow in real time the student who reads a text with the help of a cursor. The purpose of this treatment is to create a motivating experience for students, so as to help them read more. This allows students to overcome the cognitive fatigue related to reading over a long period of time. In addition to real-time tracking, errors made by students are also detected. They will not all be reported to them, the main purpose being to read. Even if they are not reported to students, they are recorded in the raw learning traces.

By accepting this policy, you accept collection of these audio recordings. However, the browsers request permission for Lalilo to access the microphone. So a teacher may use Lalilo without giving access to the audio data by simply refusing to let Lalilo access the microphone when the browser requests to do so. No recording will be made then, and one can use Lalilo normally, with the exception of exercises and features related to the microphone that will not be offered.

Cookies

We use "Local storage" and the browser's cookies to store session information. In particular, we stock the school code, which allows students to reconnect without entering the class code for each use, and the home use code for the same reason. We do not use it for advertising or marketing purposes.

You can check in your browser the list of cookies installed on your computer after browsing lalilo.com.

Appendix 2: Third-party applications

Google Analytics

Google Analytics is a tool to measure events coming to all sites in {} .lalilo.com (lalilo.com, app.lalilo.com, student.lalilo.com ...). Event sequences are recorded (arrival on the site, click on the registration button, click on the exercise preview button ...). This allows us to understand the use of the site and improve the user experience of our sites / platforms. We do not transmit personal information to Google Analytics. We only transmit the nature of the interaction (which button was clicked).
If preferred, one can use software to prevent the activation of Google Analytics, such as the plugin "Google opt-out".

Mixpanel

Mixpanel is a tool dedicated to the statistical analysis of behaviors. It is similar to Google Analytics in the way it works. It allows us to better understand the behaviors of our users, and to detect flaws in the user experience of our website.
Mixpanel also allows us to send emails in reaction to particular events (such as sending a welcoming email when signing up). We do send identifying information to mixpanel, for this communication purpose, including the teacher' email address when we have it.

Facebook Pixel

We use Facebook pixel. Its operation is similar to that of Google Analytics. When the user clicks on a button on the Lalilo Facebook page, it is taken into account and allows to track how the user uses the site. We use Facebook pixel to determine the impact of Facebook ads to promote Lalilo. This allows us to know how many users have registered on the platform through Facebook advertising. No identifying data is communicated from us through the Facebook pixel. We only communicate the type of event (the type of button clicked by the user).

MailChimp

MailChimp is a newsletter manager. MailChimp allows a company to manage lists of email addresses and launch email campaigns. One can unsubscribe from the newsletter by clicking the button of each email you are sent ("unsubscribe from this list"). The recipient will continue to receive non-newsletter emails, necessary for the use of the platform (CGU update, privacy policy, or other information essential to the enlightened use of the platform).

AskNicely

AskNicely is a feedback manager. AskNicely allows Lalilo to send to a set of email addresses using a questionnaire format as follows: "From 0 to 10, how much would you recommend Lalilo to another teacher?" - and to ask the recipient for written comments.
Each feedback (note and comment) is associated with the email address from which it comes. Recipients are under no obligation to respond to this solicitation (which can only happen 2 to 4 times a year maximum). One can unsubscribe by clicking on the "Unsubscribe" button at the bottom of the email.

FullStory

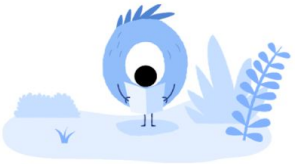
Some of the sessions are recorded on FullStory, associated with the email address of the user of the website. The first aim is to solve bugs, being able to observe them. The second purpose is to understand the users' behaviors to ensure the fluidity of use. The recorded session reproduces what the user sees in the tab on one of the subdomains of lalilo.com.

Intercom

We use Intercom as a user support tool. This is a chat, usable from lalilo.com and app.lalilo.com. It is not accessible from the student platform (student.lalilo.com). Intercom automatically retrieves the email address of the user if the teacher is logged

in. If the user is not logged in, the only information sent to Intercom is the information already provided by the user.

The third party services listed above may place cookies related to browsing history on lalilo.com. These make it possible to ensure the proper functioning of the listed services. One can check the browser to review the list of cookies installed on the computer after browsing lalilo.com.



Lalilo Inc.
400 Montgomery Street, Suite 1100, San Francisco, CA
privacy@lalilo.com / www.lalilo.com