

**MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT
VERSION (2018)**

Natick Public Schools

and

Rosetta Stone Ltd

November 15, 2018

This Massachusetts Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Natick Public Schools (hereinafter referred to as "LEA") and Rosetta Stone Ltd (hereinafter referred to as "Provider") on November 15, 2018. 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, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; 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

- 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.
- 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 Exhibit "C". 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 L E A.** 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 and if applicable to the Services, 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 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.

- 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, at LEA's own expense and subject to a binding Non-Disclosure Agreement. 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	<u>Rosetta Stone Ltd.</u>
Title	<u>Data Privacy Officer</u>
Address	<u>1621 N. Kent Street, Suite 1200</u>
Telephone Number	<u>1-800-788-0822</u>
Email	<u>Privacy.officer@rosettastone.com</u>

The designated representative for the LEA for this Agreement is:

Name	Dennis Roche
Title	Technology Director, Natick Public Schools
Address	15 West Street, Natick, MA 01760
Telephone Number	508-647-6628
Email	droche@natickps.org

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 OF MIDDLESEX COUNTY 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. **Waiver.** 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. **Electronic Signature:** 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. **Multiple Counterparts:** 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).

ARTICLE VII- 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 this to any other school district who signs the acceptance in said Exhibit.

[Signature Page Follows]


IN WITNESS WHEREOF, the parties have executed this Massachusetts Student Data Privacy Agreement as of the last day noted below.

NATICK PUBLIC SCHOOLS



Date: 11-29-18
Printed Name: Grace Magley Title: Director of Digital Learning

ROSETTA STONE LTD



Date: November 19, 2018
Printed Name: Sean Hartford Title: V.P., Controller & PAO

EXHIBIT "A"

DESCRIPTION OF SERVICES

K12 Rosetta Stone® Online Language Solutions For Schools and School Districts

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 that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
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	

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	

EXHIBIT
"C"

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

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer through its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled on the next page for the Subscribing LEA. 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 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 statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

ROSETTA STONE LTD

BY: 

Date: November 19, 2018

Printed Name: Sean Hartford

Title/Position: V.P., Controller & PAO

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's individual information is below. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DATE: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name

Title

Address

Telephone Number

Email

COUNTY OF LEA: _____

OPTIONAL:
EXHIBIT "F"

**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? x Yes ☐ No

If yes, please provide it.

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

____ NIST Framework for Improving Critical Infrastructure Security

____ Other: _____

3. Does your organization store any customer data outside the United States? Yes x No
4. Does your organization encrypt customer data both in transit and at rest? X 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: Data Privacy Officer

Contact information: PrivacyOfficer@RosettaStone.com

6. Please provide any additional information that you desire.

STUDENT RECORDS PRIVACY STATEMENT & SECURITY PLAN

Rosetta Stone Ltd.

We take the privacy of our educational clients and student users seriously, and we understand the need to safeguard personally identifiable information in records of students who access and use our web-based language and learning products and services ("Student Records") through the educational institutions, schools and school districts that we serve (our "Education Clients").

Student Records are the property of our Education Clients. We receive those Student Records solely for the purposes of delivering our products, services and commitments under our agreements with our Education Clients. We are committed to working with our Education Clients to comply with all applicable laws, rules and regulations governing the use and protection of Student Records, including the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g and its implementing regulations, and applicable state laws and statutes governing Student Records. As such, we commit to implementing and maintaining this Student Records Privacy Statement & Security Plan ("Student Records Security Plan"), which is designed to protect the security, confidentiality and integrity of Student Records that we receive from our Education Clients, and protect against unauthorized access or other anticipated threats to those Student Records.

In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.

We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records. Our products and services do not currently utilize or enable students to upload student-generated content, but if we offer such functionality in the future, we will work in good faith with our Education Clients to develop processes to address requests by students for the transfer of such content generated by the student during the service term.

We use Student Records only for the purpose for which they are provided to us or as otherwise authorized in the applicable agreement with the Education Client. We do not sell Student

Records or use them for targeted marketing or similar commercial purposes, and do not authorize others to do so. We do not disclose Student Records to unauthorized third parties without the permission from the Education Client, unless required by statute, agency or court order, subpoena or similar compulsory legal process.

If a parent, legal guardian or student contacts us with a request to review the user's Student Records or correct erroneous information, or if an agency, court, law enforcement or other entity contacts us and requests access to Student Records, we will (unless prohibited by writ or compulsory legal process) promptly notify an authorized representative of the applicable Education Client and use reasonable and good faith efforts to assist the Education Client in fulfilling such requests, as required by law and directed by the Education Client.

If we determine that an incident involving Student Records has occurred that would be subject to reporting under applicable federal or state law, we will take prompt and appropriate steps to mitigate the incident and/or further impact to the Student Records; provide notice to the affected Education Client promptly and without unreasonable delay; and work with the affected Education Client to provide information and assistance necessary to comply with any notification to parents, legal guardians, students, or other persons or entities, as required under applicable law.

Following expiration or termination of the agreement under which the Education Client purchased access to our web-based products or services and upon receipt of written direction from the Education Client, we will take steps to destroy, or if agreed, return the Student Records in our possession to the Education Client within a commercially reasonable period of time. For clarity, data or data elements within Student Records generated by use of our products or services that are in aggregate form or that are de-identified or anonymized (i.e., where direct and indirect personally identifiable identifiers that would associate the data or element with an individual student or user have been removed), may be retained and used for product and service improvement, statistical analysis, and/or educational research-related purposes.

This Student Records Security Plan is effective March 31, 2016. From time to time we may update this Student Records Security Plan to reflect changes to our privacy practices in accordance with changes in legislation, best practice or our products. Notice of material changes to this Student Records Security Plan will be provided to Education Clients by email to the address on file for the account, by including a notice in our invoice documentation to Education Clients, or by placing notice within our web-based products or on our website.

For questions or further information on our data privacy and security practices with respect to Student Records, please contact our privacy officer at PrivacyOfficer@RosettaStone.com.

EXHIBIT "G"
Non-Disclosure Agreement

Please see following page.

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (this "Agreement") is made between is made between the Rosetta Stone company identified in the signature block below ("Company"), and Natick Public School, a corporation, having a principal office at 13 E Central St, Natick, MA 01760 ("Recipient", "you"). For good and valuable consideration, the parties agree as follows:

1. PURPOSE. The parties contemplate (i) conducting certain reviews, discussions, presentations and/or analyses concerning the business of Company and/or, (ii) exploring the provision of employment, consulting, or other technical or professional services to Company. Company is engaged in the development of next-generation language learning software products that combine technical innovations with advances in pedagogical theory and instructional methodology (the "Product"). Company has invested significant resources in research and development for the Product. All aspects of the Product, including its design, functionality, look and feel, pedagogical theory, and instructional methodology are considered by Company to be proprietary and highly confidential. Company will disclose to you confidential information including competitively sensitive and proprietary information. You agree this represents a valuable commercial opportunity for you. Nothing in this Agreement shall require Company to disclose any of its Confidential Information.

2. DEFINED TERMS.

For purposes of this Agreement, the term "Confidential Information" means all information disclosed by Company and/or its affiliates to you (whether prepared by Company or its agents or advisors) in oral, electronic, tangible or intangible form (together with notes, analyses, work papers, compilations, comparisons, studies or other documents prepared by Company) concerning the products, services, technology, and business of Company that is either identified by Company before its disclosure to you as being confidential or that would be understood by the parties, exercising reasonable business judgment, to be confidential (including, but not limited to, all aspects of the Product and any information on other released or unreleased Company software products, online services, business methods, strategies and clients, business and financial information and models, names of customers or partners (whether potential or existing), cost and pricing data, market and/or financial projections, and proposed business deals).

Confidential Information does not include information that (i) is now or subsequently becomes generally available to the public through no fault or breach on the part of Recipient, (ii) can be demonstrated by Recipient to have had rightfully in its possession prior to disclosure to Recipient by Discloser, or is independently developed by Recipient without the use of any Confidential Information; prior to the time of disclosure, (iii) Recipient rightfully obtains from a third party who has the right to transfer or disclose it, or (iv) is lawfully required to be disclosed to any governmental agency or is otherwise required to be disclosed by law, provided however that before making such disclosure Recipient shall give written notice, along with the asserted grounds for disclosure, and Discloser adequate opportunity to interpose an objection and/or take action to assure confidential handling of such information. In the event protection against disclosure is not obtained, Recipient shall only disclose the Confidential Information to the extent necessary to legally comply with such compelled disclosure.

3. NON-DISCLOSURE. You agree: (i) to maintain in strict confidence, and agree not to make any use of or disclose for any purpose other than the purpose set forth in Section 1, any Confidential Information that you receive, (ii) any unauthorized use of Confidential Information by any parent, subsidiary, affiliate, employee, consultant, or agent shall be deemed a material breach of this agreement, and (iii) to have all recipients of the confidential information sign, and maintain in your files, a non-disclosure in content similar to the provisions hereof, prior to any disclosure of Confidential Information.

4. ADDITIONAL SAFEGUARDS. You agree that, in addition to the foregoing obligations, you will treat and take all steps necessary to protect all Confidential Information in the same manner as you would treat and protect your own most highly confidential and proprietary information and trade secrets, and you will in no event treat the Confidential Information with less than reasonable care.

5. COPIES. You agree not to make any duplicate copies, or summaries of any printed or electronic Confidential Information, except those which are necessary for you to carry out the purpose expressly set forth in Section 1 hereof. To the extent that the Confidential Information is comprised of computer software, you agree not to copy any part of it in machine-readable or printed form or otherwise.

6. OWNERSHIP OF CONFIDENTIAL INFORMATION. All Confidential Information disclosed to you pursuant to this Agreement shall remain the sole and exclusive property of Company. You expressly acknowledge and agree that no right or license with respect to the Confidential Information or the Product is granted hereby to you, and none may be inferred from the provisions of this Agreement. Recipient agrees not to use any Confidential Information as a basis upon which to develop or have a third party develop a competing or similar product.

7. FEEDBACK. It is anticipated that you will provide suggestions, comments or other feedback to Company, regarding the Product and Company's other products, services, technology and business ("Feedback"). Feedback will not, absent a separate written agreement, create any confidentiality obligation for Company. Company will be free to use, disclose, reproduce, license or otherwise distribute and exploit the Feedback provided to it as it sees fit, entirely without obligation or restriction of any kind on account of intellectual property rights or otherwise. Without limitation of the foregoing, if you suggest new features, functionality, pedagogical techniques, or business methods that Company adopts for the Product, or any of its other products or services, these will be the sole and exclusive property of Company.

8. TERM AND TERMINATION.

(a) This Agreement will terminate upon the earlier of (i) the completion of the purpose set forth in Section 1 hereof, or (ii) the written request of either party. Upon the termination of this Agreement, the confidentiality obligations set forth hereunder will continue in effect for a period of three (3) years, from the effective date of this Agreement, except that the confidentiality obligations with respect to any information that constitutes a trade secret shall continue in effect for so long as such information remains a trade secret, and the provisions set forth in Section 6 hereof regarding ownership shall continue in effect for so long as necessary to give full effect thereto. You agree, upon termination of this agreement, to return all Confidential Information disclosed hereunder, including all originals, copies and summaries at Company's request or, at Company's option, provide written certification of your destruction of the Confidential Information.

(b) Further, the obligations to not disclose shall not be affected by bankruptcy, receivership, assignment, attachment, or seizure procedures, whether initiated by or against Recipient, by a trustee or Recipient in bankruptcy, or by the Recipient as a debtor-in-possession, or the equivalent of any of the foregoing under the law.

(c) If the parties engage in any business relationship in the future, they agree that, absent a separate written agreement, that relationship will be governed by the terms of this Agreement.

9. REMEDIES. You acknowledge that any breach of this Agreement may give rise to irreparable harm to Company for which money damages alone would not be an adequate remedy. You agree that, in addition to Company's other remedies, Company will be entitled to enforce the provisions of this Agreement by injunction and seek other equitable relief, to remedy any threatened or actual breach, without the necessity of posting bond or proving the inadequacy of money damages as a remedy. If Company employs attorneys to enforce its rights under this Agreement, Company shall be entitled to recover reasonable attorneys' fees and costs if it prevails.

10. GOVERNING LAW; JURISDICTION. This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia without reference to its provisions of conflict of laws. The parties expressly agree that any controversy, claim or dispute arising under or relating to this Agreement, including, without limitation, the existence, validity, interpretation, performance, breach or termination thereof, shall be brought and decided in the state or federal courts of the Commonwealth of Virginia. The parties expressly waive any objections on grounds of forum non conveniens, venue or personal jurisdiction to proceedings in Virginia.

11. AMENDMENT; ASSIGNMENT. This Agreement may not be amended in any respect whatsoever except by a further agreement, in writing, fully executed by the authorized representatives of each of the parties. This Agreement will be binding, and inure to the benefit of the parties and their affiliates, heirs, successors and permitted assigns. The provisions of this Agreement may not be assigned, sold, or otherwise transferred, in whole or in part, without the prior written consent of Company.

12. LIMITED EFFECT. This Agreement does not create any obligation on either party to enter into any transaction between them, and each party reserves the right, in its sole discretion, to terminate the discussions contemplated herein upon written notice to the other party.

13. CONCLUDING PROVISIONS.

- (a) This Agreement and any amendments hereto may be executed in one or more counterparts.
- (b) If any provision of this Agreement, or the application thereof, shall, for any reason and to any extent, be found invalid or unenforceable, the remainder of this Agreement and the application of such provision to other circumstances will not be affected thereby, but rather will be enforced to the maximum extent permissible under applicable law, so long as such enforceability does not materially adversely affect the mutual rights and obligations of the parties hereunder.
- (c) This Agreement represents the entire agreement and understanding of the parties regarding the subject matter hereof, and terminates and supersedes all prior undertakings, or agreements on the subject matter hereof.
- (d) Either party's failure to insist in any one or more instances upon strict performance by the other party of any of the terms of this Agreement shall not be construed as a waiver of any of the terms of this Agreement.
- (e) Headings used in the Agreement are provided for convenience only, and shall not be used to constitute meaning or intent.
- (f) Recipient agrees not to disclose its participation hereunder, the existence or terms and conditions of this Agreement, or the fact that discussions are being held with Company.
- (g) Any notice required or given in connection with this agreement, shall be in writing, and shall be given to the appropriate party by personal delivery, or by certified mail, postage prepaid, return receipt, or recognized overnight delivery service, with delivery signature.
- (h) All Confidential Information is provided "as-is". Company makes no warranties, express, implied, or otherwise, regarding its accuracy, completeness or performance, non-infringement of third party rights, or its merchantability, or fitness for a particular purpose.
- (i) The parties represent, warrant and covenant that they have the full right and authority to enter into this Agreement and perform its obligations hereunder, that all required corporate approvals and authorizations have been obtained, and that upon signature by its authorized representative below, the Agreement shall have been duly executed and be legally binding upon the parties in all respects.

IN WITNESS WHEREOF, the parties hereto have executed and delivered this Agreement.

Rosetta Stone LTD
135 W. Market St., Harrisonburg, VA 22801 USA

Date: *November 19, 2018*

Signed 

Print Name: Sean Hartford

Title: VP Controller and PAO

RECIPIENT:
Natick Public Schools

Date:

Signed _____

Print Name:

Title:

Address:

Phone:

Fax: