

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

Wrentham Public Schools

and

Heinemann, a division of Greenwood Publishing Group, LLC

March 26, 2020

This Massachusetts Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Wrentham Public Schools (hereinafter referred to as “LEA”) and Heinemann, a division of Greenwood Publishing Group, LLC (hereinafter referred to as “Provider”) on March 26, 2020. 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 may, by signing the "General Offer of Privacy Terms" (Exhibit "E"),, agree to allow the LEA to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of this 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

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

- 3 **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit "B".
- 4 **DPA Definitions.** The definition of terms used in this DPA is found in 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 LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. In order to assist pupils in retaining possession and control of their own pupil-generated content, upon written request from the LEA, Provider will cooperate with LEA in the timely transfer of identified pupil-generated content to LEA, or if practicable, to a non-Provider personal account. Non-LEA requests to Provider for pupil-generated content from students and/or parents/guardians will be sent to LEA and not acted upon by Provider. Notwithstanding the foregoing, Provider retains all right, title and interest in and to any and all of Provider's software, materials, tools, forms, documentation, training and implementation materials and intellectual property (collectively, "Provider Materials".) Provider grants to LEA a personal, nonexclusive license to use the Provider materials for its own non-commercial, incidental use as set forth in the end user license agreement accompanying such software and as contemplated herein.
- 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, or to establish a non-Provider, personal account for pupil-generated content. Provider shall cooperate and respond within ten (10) calendar days to the LEA's written request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary, or for pupil-generated content in order to establish a non-Provider, personal account. 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, cooperate with the LEA in the transfer of identified pupil-generated content to LEA or if practicable, to a non-Provider personal account. Alternatively, the Provider will provide Student Data in another format within thirty (30) days at the LEA's written request.

- 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, unless prohibited by law, regulation, or lawful court order, 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, except for Subprocessors necessary to provide services hereunder, 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 be bound by provisions at least as protective as 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 and Service Agreement 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 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, PPR, , 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 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 Services contracted for under this DPA.
5. **Disposition of Data**. Upon written request, 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 according to a schedule and procedure as the Parties may reasonably agree. If Provider is directed by LEA to transfer said data to LEA or LEA's designee, Provider shall do so within sixty (60) days of the date of written direction 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 promptly provide the LEA with any specified portion of the Student Data within ten (10) 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 commercially reasonable data security measures, consistent with industry standards and commercially reasonable technology practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below.
 - . These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall exercise commercially reasonable practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data. 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. 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 are reasonably designed to meet industry standard practices in the transfer or transmission of any data, including restricting the viewing or access of data to the 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 provide the Services and 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 reasonably consistent with the terms of this Article V. Provider shall periodically conduct or review assessments of Subprocessors to determine the adequacy of their security program.
 - h. **Ongoing Risk Assessment.** Provider further acknowledges and agrees to conduct ongoing 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 written request from the LEA, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will reasonably cooperate 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 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 Provider. Such audits shall be made no more than once per year, during normal business hours, and not take longer than one (1) business day. Such audits shall be subject to scheduling according to the mutual convenience of the Parties. 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, and such unauthorized access is caused by the fault of the Provider and not that of LEA or its agents, 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, if practicable, under the following headings or equivalent organizational structure: “What Happened,” “What Information Was Involved,” “What We Are Doing,” 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, if practicable, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.

- ii. To the extent feasible, 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, if practicable:
- i. Information about what the agency has done to protect individuals whose information has been breached.
 - 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 commercially reasonable 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 containing non-proprietary and non-confidential information.
 - f. Upon LEA's written request, Provider shall assist the LEA in the LEA's notification of 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, provided that Provider has been given written notice of such material breach and has had a reasonable period of time to remedy such breach prior to termination.

3. **Effect of Termination Survival.** If the DPA is terminated, then upon written request by LEA, the Provider shall destroy or dispose of 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	Heinemann, a division of Greenwood Publishing, LLC_____
Title	Attention: Lori Lampert_____
Address	361 Hanover Street, Portsmouth, NH 03801_____
Telephone Number	603-431-7894, ext 1115_____
Email	lori.lampert@heinemann.com_____

The designated representative for the LEA for this Agreement is:

Sean Ahern, Director of Technology
 aherns@wrenthamschools.org
 508-384-5430 x2010
 Wrentham Public Schools
 120 Taunton Street, Wrentham, MA 02093

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 NORFOLK 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 disposal 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 DPA to any other school district LEA who signs the acceptance in said Exhibit. The General Offer is limited by the terms and conditions described herein.

[Signature Page Follows]

WRENTHAM PUBLIC SCHOOLS

Sean A Ahern
Sean A Ahern (May 11, 2020)

May 5, 2020

Date: _____

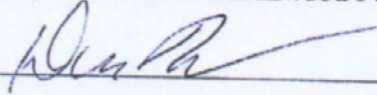
Sean A Ahern

Printed Name: _____

Director of Technology

Title: _____

Heinemann, a division of Greenwood Publishing Group, LLC



Date: March 23, 2020 _____

Printed Name: Diana Tomasyan _____

Title: Sr. Director of Opertions _____

Fountas & Pinnell Classroom, literacy instruction.

The service we provide is a reading assessment specific database for teachers to: input and store student reading assessment records, run reports on the assessments per student, group of students or class (typically to see student growth over time), allow administrators to see what teachers have placed into the system, and allow administrators to run reports at a 'higher level' (grade, school, district) on the assessment scores (typically to see student growth/class growth/school growth over time)

Heinemann Fountas & Pinnell Online Data Management System (ODMS)

The Online Database Management System (ODMS) is designed to work in conjunction with Teachers who have purchased Fountas & Pinnell reading product(s) and who want to store reading assessments in a secure database.

Our ODMS allows teachers to they themselves input the grade, names and assessment scores (level, accuracy, fluency, comprehension, reading rate, writing about reading) of any and all students that they want to store the reading assessment records of.

In addition, to assist teachers if the teacher/school wishes we also have fields for Student ID, School Year, School name, Teacher name, Grade level, Class name, Student gender, IEP, Other Reading assessment comments, Free lunch designation, and a 'free form' comment item. These additional items are available at the users discretion and do not need to be used.... Different schools use different fields.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Met	IP Addresses of users; Use of cookies;	Not used
	Other application technology metadata	Not used
Application Use Statistic	Metadata on user interaction with applic	Not used
Assessment	Standardized test scores	Not used
	Observation data	If Teachers choose to enter the information
	Other assessment data – Please specify	If Teachers enter the information Our ODMS allows teachers to they themselves input the grade, names and assessment scores (level, accuracy, fluency, comprehension, reading rate, writing about reading) of any and all students that they want to store the reading assessment records of. In addition, to assist teachers if the teacher/school wishes we also have fields for Student ID, School Year, School name, Teacher name, Grade level, Class name, Student gender, IEP, Other Reading assessment comments, Free lunch designation, and a 'free form' comment item. These additional items are available at the users discretion and do not need to be used.... Different schools use different fields.
Attendance	Student school (daily) attendance data	Not used
	Student class attendance	
Communications	Online communications that are captured (emails, blog entries)	Not used
Conduct	Conduct or behavioral data	Not used
Demographics	Date of Birth	If Teachers choose to enter the information
	Place of Birth	Not used
	Gender	If Teachers choose to enter the information
	Ethnicity or race	If Teachers choose to enter the information
	Language Information (native, preferred primary language spoken by student)	If Teachers choose to enter the information
	Other demographics – Please specify:	IEP, Free Lunch...again if Teachers choose to enter the information
Enrollment	Student school enrollment	Yes
	Student grade level	Yes
	Homeroom	If Teachers choose to enter the information
	Guidance counselor	If Teachers choose to enter the information
	Specific curriculum	If Teachers choose to enter the information
	Year of graduation	NO
	Other enrollment information –	Has a "notes" area so anything a Teacher chooses to enter

	Elements	Check if used by your system
	Please specify:	
Parent/Guardian Contact Information	Address	NO
	Email	NO
	Phone	NO
Parent/Guardian ID	Parent ID number (created to link parents to students)	NO
Parent/Guardian Name	First and/or Last	NO
Schedule	Student scheduled courses	NO
	Teacher names	Reading Teacher Class name
Special Indicator	English language learner information	If Teachers choose to enter the information
	Low income status	NO
	Medical alerts	NO
	Student disability information	If Teachers choose to enter the information
	Specialized education services (IEP or 504)	If Teachers choose to enter the information
	Living situations (homeless/foster care)	If Teachers choose to enter the information
	Other indicator – Please specify:	
Student Contact Information	Address	NO
	Email	NO
	Phone	NO
Student Identifiers	Local (School district) ID number	Many schools use a student ID
	State ID number	NO
	Vendor/App assigned student ID number	YES, the database assigns a number (in the background) to each student - Teachers / users never know this number. It is used for connecting tables in the database
	Student app username	NO
	Student app passwords	NO
Student Name	First and/or Last	YES
Student in App Performance	Program/application performance (typing program-student types 60 wpm; reading program-student reads below grade-level)	YES as entered by the Teacher
Student Program Members	Academic or extracurricular activities a student may belong to or participate in	If Teachers choose to enter the information
Student Survey Responses	Student responses to surveys or questionnaires	NO

Check it out by your system		
Student Work	Student generated content; writing, pic etc.	NO student use in system at all
	Other student work data – Please specify	NO
Transcript	Student course grades	Reading Assessment scores
	Student course data	Reading Assessment scores
	Student course grades/performance scores	Reading Assessment scores
	Other transcript data – Please specify:	NO
Transportation	Student bus assignment	NO
	Student pick-up and/or drop-off location	NO
	Student bus card ID number	NO
	Other transportation data – Please specify	NO
Other	Please list each additional data element stored, or collected by your application	<p>Our ODMS allows teachers to they themselves input the grade, names and assessment scores (level, accuracy, fluency, comprehension, reading rate, writing about reading) of any and all students that they want to store the reading assessment records of.</p> <p>In addition, to assist teachers if the teacher/school wishes we also have fields for Student ID, School Year, School name, Teacher name, Grade level, Class name, Student gender, IEP, Other Reading assessment comments, Free lunch designation, and a 'free form' comment item. These additional items are available at the users discretion and do not need to be used.... Different schools use different fields.</p>

System is designed specifically for Teacher and administrator use.

No student or parent use.

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.

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 (but specifically excludes DII):

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

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.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

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 as amended herein.

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.

[Name or District or LEA] directs Heinemann, a division of Greenwood Publishing Group, LLC, 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