January 21, 2021

DATA PRIVACY AGREEMENT

RECITALS

WHEREAS, in this Data Privacy Agreement ("DPA") Accelerated Learning Inc., with its principal offices located at 5177 Richmond Ave; Ste 1025, Houston TX 77056
is referred to as "Provider" and Wood Dale School District 7, DuPage County, Illinois, a local education agency ("LEA") is referred to as LEA;

WHEREAS, the Provider has agreed to provide the Local Educational Agency ("LEA") with services pursuant to a contract ("Customer Services Agreement") to which this DPA is attached. A copy of the Customer Services Agreement shall be posted on the District's website per the requirements of the Student Online Personal Protection Act; and

WHEREAS, in order to provide the Services described in the Customer Services Agreement, the Provider may receive and the LEA may provide data that are covered by several federal and Illinois statutes, among them: the Family Educational Rights and Privacy Act of 1974 ("FERPA"), 12 U.S.C. 1232g; the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/1 et seq.; the 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 Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/1 et seq; and the Personal Information Protection Act ("PIPA"), 815 ILCS 530/1 et seq.; and

WHEREAS, the Parties wish to enter into this DPA and incorporate it into the attached Customer Services Agreement to ensure that the Customer Services Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

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 transmitted to or made available to Provider from or through the LEA pursuant to the Customer Services Agreement, including compliance with all applicable privacy statutes, including the FERPA, ISSRA, PIPA, PPRA, SOPPA, and COPPA. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the control and supervision of the LEA for the DPA purposes detailed herein, though Provider shall remain as an independent contractor.

Nature of Services Provided. In performing the services under the Customer Services Agreement, Provider is likely to have access to confidential "school student records" and "education records" as defined in FERPA and ISSRA and "personally identifiable information" ("PII"). Provider is providing the following services to the LEA: Wood Dale School District 7.

2. **DPA Definitions**. The definition of terms used in this DPA shall be as follows, with any conflict between this DPA and the Customer Services Agreement being resolved with this DPA prevailing over the Customer Services Agreement:

NIST 800-63-3: 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 and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations and Assessments
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	Geolocation

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 or Student 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.

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 identifiers, search activity, photos, voice recordings or geolocation. Student Data shall constitute Pupil Records for the purposes of this Agreement.

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 the Customer Services Agreement is and will continue to be the property of and under the control of the LEA. The Parties agree that as between them, all rights, including all intellectual property rights in and to the data and records, including but not limited to Student Data or any other Pupil Records, contemplated per the Customer Services Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and ISSRA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of student data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Third Party Request**. Should a Third Party, including law enforcement 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 Student Data directly from the LEA. Provider shall notify the LEA at least five business days in advance of complying with a compelled disclosure to a Third Party unless legally prohibited.

3. **No Unauthorized Use**. Provider shall not use Student Data purposes other than as explicitly specified in the Customer Services Agreement.

ARTICLE III: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all Illinois and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, ISSRA, PPRA and PIPA (the "Privacy Laws").

2. **Authorized Use**. The data shared pursuant to the Customer Services Agreement, including unique identifiers, shall be used for no purpose other than the Services stated in the Customer Services Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Third Parties**. Provider shall not share Student Data with any third party, subcontractor, or affiliate without express written permission from the LEA. Provider shall require all subcontractors, affiliates, employees, and agents who have access to Student Data to comply with all applicable provisions the Privacy Laws with respect to the data shared under the Customer Services Agreement and with the terms of this DPA. Provider shall provide the LEA a list of any third parties or affiliates to whom Provider has shared, is sharing, or will share Student Data for purposes authorized under the Customer Services Agreement. This list shall be updated at least twice annually before January 1 and before July 1 of each year the Customer Services Agreement is in effect.

4. **No Disclosure**. Provider shall not disclose any data obtained under the Customer Services Agreement in a manner that could identify an individual student to any other entity except as authorized by the Customer Services Agreement. Deidentified information may be used by Provider for the purposes of development and improvement of Provider's products and services.

5. **Disposition of Data**. Provider shall transfer to the LEA all personally identifiable information ("PII") obtained under the Customer Services Agreement when it is no longer needed for the purpose for

which it was obtained and dispose of such data from its own systems within 45 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Customer Services Agreement authorizes Provider to maintain personally identifiable data obtained under the Customer Services Agreement 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) permanently 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. This obligation shall survive the termination of the Customer Services Agreement.

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, advertising, or other commercial efforts by the Provider or any third party; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA.

7. **Business Transfer**. In the event any merger, sale of Provider's assets, financing or acquisition of all or a portion of Provider's business to another company, user information shall not be transferred to or acquired by a third party, unless the third party adopts this Agreement and the LEA gives express written consent to the transfer of user information.

ARTICLE IV: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures 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 meet industry standard practices to 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 its employees or contractors that are performing the Services.

   b. **Security Protocols**. Provider shall maintain all data obtained or generated pursuant to the Customer Services Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Customer Services Agreement, except as necessary to fulfill the purpose of data requests by LEA.

   c. **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.

   d. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are secure and accessible only to authorized users. Provider shall host data pursuant to the Customer Services Agreement in an environment using a firewall that is periodically updated according to industry standards.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall promptly provide notification to LEA of the incident. Provider shall adhere to the following:

   a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the following information: "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 Provider's Representative from whom additional information may be obtained.

      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 shall also include any of the following:

      i. Information about what the Provider 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. Unless the breach is the fault of the LEA, the Provider shall indemnify the LEA for any costs and damages the LEA incurs investigating or remediating the breach, including but not limited to:

      i. Notifying parents of those students whose Student Data was compromised;

      ii. Notifying regulatory agencies and/or law enforcement when required by law;

      iii. Providing credit monitoring for students whose Student Data was exposed that a reasonable person would believe could impact his or her credit or financial security;

      iv. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and

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

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Customer Services Agreement or so long as the Provider maintains any Student Data.

2. **Effect of Termination Survival**. If the Customer Services Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to this DPA.

3. **LEA's Website Posting.** No later than July 1, 2021, the LEA shall post this DPA and the Customer Services Agreement on the LEA's website.

4. **Entire Agreement**. This DPA and its accompanying Customer Services Agreement 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.

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

6. **Conflict**. In the event of any conflict between the terms of this DPA and the Customer Services Agreement, the requirements and terms of this DPA shall prevail.

Signature:	Don Keeler
Printed Name:	Don Keeler
Title:	CTO
Date:	1/25/2021