

STUDENT DATA SHARING AGREEMENT

INCLUDING RESEARCH AND PREDICTIVE VALIDITY STUDY TERMS

Sapulpa Public Schools

(SCHOOL DISTRICT)

and

Amira Learning, Inc.

(PROVIDER)

This Student Data Sharing Agreement ("DSA") is entered into on the date of full execution (the "Effective Date") by and between

Sapulpa Public Schools (the "LEA"), located at:

511 E Lee Ave

ACCOUNTS PAYABLE, Sapulpa, OK, 74066-4308

(School District Address)

and **Amira Learning, Inc.** (the "Provider"), located at 490 Post St., Suite 500, PMB 2538, San Francisco, CA 94102.

WHEREAS, the Provider is providing educational and digital services to the LEA;

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

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

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

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

2. The authorized signatory of the LEA agrees to Provider's Privacy Policy and [Terms and Conditions](#). In the event there is conflict between the terms of this DSA and any other writing, including, but not limited to, the Service Agreement and Provider Terms and Conditions or Privacy Policy, the terms of this DSA shall control.
3. This DSA shall stay in effect for the term of the LEA's subscription to Amira unless earlier terminated as provided herein.
4. The services to be provided by Provider to the LEA pursuant to this DSA are detailed in Exhibit "A" (the "Services").
5. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DSA is:

Name:

Title:

Phone:

Email:

The designated representative for the Provider for this DSA is:

Name: Pete Jungwirth

Title: Chief Technology Officer

Phone: 866-883-7323

Email: orders@amiralearning.com

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

LEA: Sapulpa Public Schools

BY: _____ **Date:** _____

Printed Name: _____ **Title:** _____

PROVIDER: Amira Learning, Inc.

BY:

Date:

Printed Name: Pete Jungwirth Title: Chief Technology Officer

STANDARD CLAUSES

ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DSA.** The purpose of this DSA is to describe the duties and responsibilities to protect Student Data, including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA with respect to its use of Student Data. The LEA agrees that the Provider is a School Official acting on the LEA's behalf.
- 2. Student Data to Be Provided.** In order to perform the Services described above, the LEA shall provide Student Data as identified in the Schedule of Student Data, attached hereto as Exhibit "B".
- 3. DSA Definitions.** The definition of terms used in this DSA is found in Exhibit "C". In the event of a conflict, definitions used in this DSA shall prevail over terms used in any other writing, including, but not limited to, the Service Agreement, Terms of Service, Privacy Policies, etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 1. Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DSA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- 2. Parent Access.** To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of the Services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request, or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data

accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** The LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 C.F.R. § 99.31(a)(1)), the LEA shall include a specification of criteria for determining who constitutes a "School Official" and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** The LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data and to obtain consents as required by governing law.
4. **Unauthorized Access Notification.** The LEA shall notify Provider promptly of any known unauthorized access. The LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal and state laws and regulations pertaining to data privacy and security, including FERPA at 20 U.S.C. § 1232g (34 C.F.R. Part 99); COPPA at 15 U.S.C. §§ 6501-6506 (16 C.F.R. Part 312); PPRA at 20 U.S.C. § 1232h; the applicable student data privacy laws and regulations of the State of _____; and any other applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit "A", the purposes authorized in Section 6 of this Article IV, or as stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DSA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DSA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data, other than as directed or permitted by the LEA or this DSA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DSA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data.** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purposes and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DSA or any request by the LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer De-Identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Consent to Use of Data for Educational Purposes and Product Improvement.** The LEA hereby consents to, and authorizes, Provider's use of Student Data for the following purposes, each of which the Parties agree constitutes a legitimate educational interest and use on behalf of the LEA: (1) to provide, deliver, maintain, support, and secure the Services; (2) for adaptive learning and customized or personalized student learning, including generating individualized instruction, practice, feedback, and personalized learning recommendations for students; (3) to generate assessments, screenings, reports, and analytics for the LEA, its teachers, and administrators, and, where applicable, for parents and legal guardians; (4) to maintain, develop,

support, evaluate, diagnose, and improve Provider's educational products and services, including improving and training the accuracy and efficacy of Provider's reading assessment, speech recognition, and instructional models; and (5) to demonstrate the effectiveness of the Services. Where Student Data is used pursuant to subsections (4) or (5), Provider shall (a) apply the security and confidentiality protections of this DSA to all such data; (b) De-Identify such data prior to any use or disclosure outside of Provider and its Subprocessors; and (c) not use such data for Targeted Advertising or to Sell Student Data. Nothing in this section shall be construed to limit the Provider's use of De-Identified Data as set forth in Section 5 of this Article IV.

7. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within thirty (30) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DSA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II, Section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as Exhibit "D". If the LEA and Provider employ Exhibit "D", no further written request or notice is required on the part of either Party prior to the disposition of Student Data described in Exhibit "D".
8. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian, or group, for any purpose other than providing the Services to the LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services, or from otherwise using Student Data as permitted in this DSA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of the Services to the LEA. The Provider will cooperate

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

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

4. Data Breach. In the event of an unauthorized release, disclosure, or acquisition of Student Data, the Provider shall provide notification to the LEA's designated representative immediately, but not longer than seventy-two (72) hours after confirmation of the incident, so that breach notification can occur as required by applicable state law. Such notification will include a copy of a forensic report describing the data breach, including an account of the data that may have been compromised, and a description of the corrective actions that will be undertaken.

The notice shall be clear and conspicuous and include a description of: (1) the incident in general terms; (2) the type of personal information that was subject to unauthorized access and acquisition; (3) the general acts to protect the personal information from further unauthorized access; (4) a telephone number that a person may call for further information and assistance, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

The security breach notification shall also include, at a minimum: (1) the name and contact information of the reporting LEA; (2) a list of the types of personal information believed to have been the subject of the breach; (3) the date or estimated date or date range of the breach, plus the date of the notice; (4) whether the notification was delayed due to a law enforcement investigation; and (5) a general description of the breach incident.

Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including the required responsibilities and procedures for notification and mitigation of any such data breach.

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 the LEA, upon request, with a summary of said written incident response plan.

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

ARTICLE VI: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DSA, they may do so by mutual written consent.
2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall dispose of all of the LEA's Student Data pursuant to Article IV, Section 7.
3. **Priority of Agreements**. This DSA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DSA. In the event there is conflict between the terms of the DSA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DSA shall apply and take precedence.
4. **Entire Agreement**. This DSA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DSA may be amended and the observance of any provision of this DSA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties.
5. **Execution in Counterparts; Electronic Signatures**. This Agreement may be executed in multiple counterparts, each of which shall be deemed a duplicate original, but all of which taken together shall constitute one and the same instrument. The submission of a signature page transmitted by an electronic signature service (e.g., DocuSign) shall be considered an "original" signature page for purposes of this Agreement.
6. **Severability**. Any provision of this DSA 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 DSA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction.

- 7. Governing Law; Venue and Jurisdiction.** THIS DSA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF _____, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION OF THE STATE AND FEDERAL COURTS FOR THE COUNTY OF _____ FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DSA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
- 8. Successors Bound.** This DSA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation, or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DSA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DSA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DSA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
- 9. Authority.** Each Party represents that it is authorized to bind to the terms of this DSA, 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.
- 10. Waiver.** No delay or omission by either Party to exercise any right hereunder shall be construed as a waiver of any such right, and both Parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Part 1: Educational Services

Amira Learning licenses include access to Amira ISIP Assess and Amira Tutor. Amira Tutor is an AI-based literacy platform that listens to students read aloud, provides real-time feedback and coaching, and generates detailed reports on reading accuracy, fluency, and comprehension. Amira ISIP Assess includes screening, benchmarking, and progress-monitoring tools aligned with current research in the science of reading, including frameworks such as the Active View of Reading and the Multiple Deficit Model. These approaches support early identification of reading difficulties, including indicators of dyslexia, and provide actionable data for targeted instruction.

Participating schools will receive access to Amira ISIP Assess and Tutor for all students in grades _____, along with teacher and staff training, implementation support, and access to student-level data and reporting tools. The platform is designed to support core instruction as well as targeted intervention, while expanding the ability of teachers to provide individualized reading practice and feedback to students.

Part 2: Research and Predictive Validity Study

In addition to the educational services described in Part 1, Provider and the LEA are collaborating on a research study to evaluate the predictive validity of Provider's reading and mathematics assessments in relation to state summative assessment outcomes (the "**Study**"). The purpose of the Study is to generate evidence of the relationship between student performance on Amira ISIP Assess (reading) and ISIP Math and student performance on state summative assessments, and to support the calibration and norming of Provider's assessment instruments.

To support the Study, the LEA will provide Provider with the following data for school years 2024–25 and 2025–26, matched by Student Testing Number (STN):

- Assessment scores (Spanning no more than grades K–8 mathematics and/or reading); and
- Student Testing Numbers (STNs) for the purpose of linking LEA assessment records to Provider's existing assessment data.

Provider will use the data provided under this section, together with Amira assessment data already collected through the Services, solely for the research purposes described herein and for demonstrating the effectiveness of the Services as authorized in Article IV, Section 6(5) of this DSA. All Student Data protections, security requirements, and use limitations set forth in this DSA apply equally to the data provided under this section. Any publication or external presentation of

findings from the Study that names or identifies the LEA shall require the LEA's prior written approval pursuant to Article IV, Section 5 of this DSA.

EXHIBIT "B"**SCHEDULE OF STUDENT DATA**

The following categories and elements of Student Data are collected, used, or processed by the Provider's system in connection with the Services:

Part 1: Data Collected Through Educational Services

Category of Data	Elements
Application Technology Metadata	IP addresses of users, use of cookies, browser user agent
Application Use Statistics	Metadata on user interaction with application
Assessment	Observation data (reading assessment, screening, benchmarking, and progress-monitoring data generated by the Services)
Demographics	Language information (native or primary language spoken by student)
Enrollment	Student school enrollment; Student grade level; Class enrollment
Schedule	Teacher names
Student Identifiers	Local (school district) ID number; State-assigned student ID number; Provider/app-assigned student ID number; Student app username; Student app passwords
Student Name	First and/or last name
Student In-App Performance	Program/application performance (e.g., student reading level, accuracy, fluency, and comprehension measures generated by the Services)

Part 2: Data Provided by LEA for the Research Study

The following additional categories of Student Data will be provided by the LEA to support the Research and Predictive Validity Study described in Part 2 of Exhibit "A":

Category of Data	Elements
Assessment Data	Non-Amira Reading and/or Math Assessment Scores, for a maximum range of grades K-8
Student Identifiers	Student Testing Numbers (STNs) for the purpose of linking LEA assessment records to Provider assessment data

The Provider does not collect or process Student Data categories or elements other than those identified above. The Provider will notify the LEA and obtain any required consent or amendment to this DSA before collecting any additional categories of Student Data.

EXHIBIT "C"

DEFINITIONS

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

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

LEA: For purposes of this DSA, the term "LEA" means the school district identified on the signature page of this DSA that is providing Student Data to the Provider in connection with the Services.

Metadata: Means information that provides meaning and context to other data being collected, including, but not limited to: date and time records and purpose of creation. Metadata that has been stripped of all direct and indirect identifiers is not considered personally identifiable information.

Operator: Means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes.

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

School Official: For the purposes of this DSA and pursuant to 34 C.F.R. § 99.31(a)(1)(i)(B), a School Official is a contractor that: (1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) is subject to 34 C.F.R. § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by the LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DSA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

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

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Sapulpa Public Schools directs Provider to dispose of data obtained by Provider
(LEA Name)

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

1. Extent of Disposition.

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

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

2. Nature of Disposition.

Disposition shall be by destruction or deletion of data.

Disposition shall be by transfer of data. The data shall be transferred as follows:

3. Schedule of Disposition. Data will be disposed of by the following date:

As soon as commercially practicable

By: _____

4. Signature.

Authorized Representative of LEA

Date

5. Verification of Disposition of Data.

Authorized Representative of Provider

Date

EXHIBIT "E"**DATA SECURITY REQUIREMENTS****Adequate Cybersecurity Frameworks**

The Provider has implemented and maintains an adequate cybersecurity program based on the following nationally recognized cybersecurity frameworks ("Cybersecurity Frameworks"), which protect digital learning ecosystems and were chosen based on a set of guiding cybersecurity principles:

Maintaining Organization/Group	Framework(s)
National Institute of Standards and Technology (NIST)	NIST SP 800-53; Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF); Special Publication 800-171
American Institute of Certified Public Accountants (AICPA)	Systems and Organization Controls (SOC 2)

Any exclusions, variations, or exemptions to the identified Cybersecurity Frameworks, and any additional security programs and measures that augment or are in addition to the Cybersecurity Frameworks, are detailed in an attachment to this Exhibit "E".