

STUDENT DATA SHARING AGREEMENT

This Student Data Sharing Agreement (“**DSA**”) is entered into on the date of full execution (the “Effective Date”) by and between Amira Learning, Inc., headquartered at 490 Post St., Suite 500, PMB 2538, San Francisco, CA 94102 (“**Amira**” or the “**Provider**”), and the School District or Local Education Agency (the “**LEA**”) named in the applicable purchase order (“**PO**”). Provider and LEA are each referred to as a “Party” or collectively as the “Parties.”

WHEREAS, the Provider offers educational or digital services to the LEA as described in detail in **Exhibit A** attached hereto (the “**Services**”) subject to Provider’s Terms and Conditions available at <https://amiralearning.com/amira-terms> (the “**Terms**”);

AND 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 any other applicable student data privacy laws and regulations, including applicable state-specific laws and regulations (collectively, the “**Student Privacy Laws**”);

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

1. KEY DEFINITIONS

- 1.1 “**Data Breach**” means an unauthorized release, access to, disclosure, or acquisition of Student Data that compromises the security, confidentiality, or integrity of Student Data maintained by the Provider in violation of applicable law.
- 1.2 “**De-Identified Data**” means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular student. De-Identified Data does not constitute Student Data under this DSA.
- 1.3 “**Education Records**” shall have the meaning given to such term in FERPA.
- 1.4 “**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.
- 1.5 “**Student Data**” means any data (1) collected by the Provider on behalf of the LEA or (2) provided by the LEA or its users, students, or students’ parents/guardians to the Provider, where such data is descriptive of a student including, but not limited to, information in the student’s Education Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data shall include (a) “**personally identifiable information**” or an equivalent term as defined in the Student Privacy Laws, and (b) information that provides meaning and context to other data being collected (“**Metadata**”). Student Data constitute Education Records under the Student Privacy Laws. The categories of Student Data that Provider collects and uses are listed in **Exhibit A**, as updated from time to time upon advance

written notice to the LEA. For the avoidance of doubt, Student Data does not include De-Identified Data, including de-identified usage data regarding use of the Services.

- 1.6** “**Subprocessor**” means a party other than the LEA or Provider, who Provider uses for data collection, analytics, storage, or other services to operate and/or improve the Services, and who has access to Student Data. For the avoidance of doubt, a “Subprocessor” is the equivalent of a subcontractor.
- 1.7** “**Third Party**” means an entity or individual other than Provider, Provider’s employees or agents, the LEA, Subprocessors, a student, or a parent or legal guardian of a student.

2. PURPOSE AND SCOPE

- 2.1** **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.
- 2.2** **Role of the Parties.** The Parties agree that in performing the Services, the Provider shall be considered a school official with a legitimate educational interest in accordance with 34 C.F.R. § 99.31(a)(1). With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DSA. To the extent required under the applicable Student Privacy Laws, the Parties agree that the LEA provides consent on behalf of parents or legal guardians for the collection of Student Data in accordance with the terms of this DSA.
- 2.3** **Agreement to Terms.** The LEA acknowledges receipt of and agrees to the Terms and Provider’s Privacy Policy available at <https://amiralearning.com/amira-privacy> (the “**Privacy Policy**”). Provider has provided LEA with a COPPA Direct Notice available at <https://amiralearning.com/amira-coppa> the receipt of which LEA acknowledges. In the event of a conflict between the DSA and the Terms, Privacy Policy, or any other agreement between the Parties, the terms of this DSA shall control.
- 2.4** **Compliance with Applicable Laws.** The LEA and Provider shall comply with the applicable Student Privacy Laws, as amended from time to time. In the event of an amendment to or change to the applicable Student Privacy Laws, the LEA and Provider agree to cooperate on appropriate revisions to this DSA.

Without limiting the foregoing, the Parties acknowledge that the Services involve the collection and processing of Audio Data (as defined in Exhibit A) solely for instructional and assessment purposes authorized by the LEA. The Parties agree that Provider’s collection and processing of Audio Data under this DSA is performed by Provider in its capacity as a contractor providing services on behalf of, and under the direction and control of, the LEA — which is a local educational agency and local unit of government — and is limited to the educational purposes described in Section 5.1. Nothing in this DSA shall be construed as an acknowledgment by either Party that Audio Data constitutes biometric identifiers or biometric information as those terms may be defined under any applicable statute, nor as a waiver of any defense or exemption that may be available to either Party under applicable law.

- 2.5** **Exhibits.** The Parties may agree to incorporate by reference in this DSA such exhibits as are required by applicable Student Privacy Laws (e.g., an exhibit committing to compliance with the LEA’s Parents Bill of Rights).

3. DATA OWNERSHIP AND AUTHORIZED ACCESS

- 3.1** **Student Data Is the Property of the LEA.** As between the LEA and Provider, all Student Data is and will continue to be the property of and under the control of the LEA. The Provider acknowledges and agrees that all copies of such Student Data, 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 in the Terms, shall remain the exclusive property of the LEA.
- 3.2** **Parent, Legal Guardian, and Student Access.** To the extent required by applicable law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data or “Instructional Materials” or “Surveys” (as defined in the PPRA), request deletion of or modification to Student Data, or request delivery of a copy of Student Data. Provider shall support LEA by responding 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 held by the Provider to view or correct as necessary.
- 3.3** **Referral of Direct Requests.** Provider shall direct any request regarding Student Data to the LEA, which will address the request in accordance with the applicable Student Privacy Laws. If Provider (1) forwards a request regarding Student Data to the LEA and (2) requests the LEA’s consent to respond to such request, the LEA shall address the request for consent in a timely manner without undue delay.
- 3.4** **Law Enforcement Requests.** Should law enforcement or other government entities (each, a “Requesting Party”) 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.

4. DUTIES OF THE LEA

- 4.1** **Obligations of the LEA.** The LEA shall provide all required notices and secure all necessary consents as required under the applicable Student Privacy Laws to enable the LEA to transfer Student Data to the Provider. 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.
- 4.2** **Reasonable Precautions.** The LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

- 4.3 Unauthorized Access Notification.** The LEA shall notify Provider without undue delay upon discovery of unauthorized access to the Services or LEA's account or credentials, or any unauthorized release, access to, disclosure of, or acquisition of Student Data that compromises the security, confidentiality, or integrity of the Student Data. If requested by Provider, the LEA will assist Provider with any investigation and mitigation of such unauthorized access.

5. DUTIES OF PROVIDER

- 5.1 Authorized Use.** The Parties acknowledge and agree that the Provider shall use the Student Data for no purpose other than (1) to perform the Services identified in **Exhibit A**, (2) for the purposes authorized in this Section 5.1, (3) as authorized by LEA in the Terms or this DSA, or (4) as required by applicable law.

- a) Consent to Use of Student Data for Educational Purposes.** 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; and (3) to generate assessments, screenings, reports, and analytics for the LEA, its teachers, and administrators, and, where applicable, for parents and legal guardians.
- b) Consent to Use and Disclosure of De-Identified Data.** The LEA hereby consents to, and authorizes, Provider to derive De-Identified Data about and based on usage of the Services for the following purposes: (1) 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; (2) to demonstrate the effectiveness of the Services; (3) to assist the LEA or other governmental agencies in conducting research and other studies; (4) for research and development of the Provider's educational sites, services, or applications; (5) for adaptive learning purposes and for customized student learning; and (6) to generate aggregate summaries or statistics. Provider will not re-identify De-Identified Data or permit any Third Party or Subprocessor to re-identify De-Identified Data. 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.
- c) Processing Limitations for Audio Data.** Provider represents and warrants that with respect to Audio Data (as defined in Exhibit A): (i) Provider processes Audio Data solely as a school official with a legitimate educational interest, acting on behalf of and under the direction and control of the LEA, for the purpose of delivering the Services; (ii) Provider does not derive from Audio Data any template, mathematical model, or other representation designed to identify, authenticate, or distinguish individual persons based on vocal characteristics; (iii) Provider does not disclose Audio Data to any Third Party or Subprocessor for the purpose of enabling individual identification, speaker recognition, or voice

authentication; (iv) Provider's processing of Audio Data is limited to (A) automated speech recognition for purposes of assessing reading accuracy, fluency, and comprehension; (B) generating instructional feedback; and (C) creating De-Identified Data for product improvement in accordance with Section 5.1(b); and (v) Upon written request from the LEA, Provider will disable the collection of Audio Data for all students rostered under the LEA's account, in which case the Services will operate without voice-based assessment features.

5.2 Restrictions on Disclosure of Student Data. Provider acknowledges and agrees that it shall not disclose or sell Student Data or any portion thereof to Third Parties, except that Provider may disclose Student Data to Third Parties in response to a lawfully issued subpoena or other legal process, including to a Requesting Party, or at the direction of the LEA.

- a) **Access by Authorized Personnel.** 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, including through appropriate training on the requirements of this DSA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data.
- b) **Access by Subprocessors.** Provider shall enter into appropriate agreements with Subprocessors in order to ensure that Subprocessors protect Student Data consistent with Provider's obligations under this DSA. Subprocessors shall not be permitted to disclose Student Data to Third Parties except based on instructions of the LEA.
- c) **Disclosure of De-Identified Data.** Provider may disclose De-Identified Data to a Third Party where: (a) the Third Party agrees in writing not to attempt re-identification of the data, 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 directly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
- d) **Aggregate Summaries or Statistics.** The Parties acknowledge and agree that Provider may publish aggregate summaries or statistics about use of the Services (where summaries or statistics do not identify individuals), including as part of case studies or to market Provider's products and services.

5.3 Disposition of Student Data.

- a) **Audio Data.** Provider shall retain Audio Data only until the end of the school year in which it was collected, after which it shall be securely disposed of. Provider will consider reasonable LEA requests for alternative Audio Data retention periods. For the avoidance of doubt, this subsection does not apply to De-Identified Data derived from Audio Data in accordance with Section 5.1(b).
- b) **Other Student Data.** Provider shall retain Student Data (other than Audio Data) for the lesser of (i) the duration of the Terms, or (ii) as long as necessary to fulfill

Provider's obligations under the Terms. Upon written request from the LEA (see **Exhibit B**, attached hereto), Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data, 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 De-Identified Data or data that has been placed in a separate student account pursuant to Section 3.2 of this DSA.

- 5.4 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. For the avoidance of doubt, this section does not prohibit Provider from using Student Data (i) for any purpose permitted in this DSA and its accompanying exhibits, including without limitation Section 5.1; (ii) for adaptive learning or customized student learning (including generating personalized learning recommendations); (iii) to make product recommendations to teachers or LEA employees; or (iv) to notify account holders about new education product updates, features, or services. As used in this section, "**Targeted Advertising**" means displaying advertisements to a student where the advertisement is selected based on Student Data to predict the student's preferences or interests. "Targeted Advertising" does not include advertising to a student in response to the student's request for information or feedback.

6. DATA PROVISIONS

- 6.1 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.
- 6.2 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 a non-disclosure 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.
- 6.3 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. Provider maintains SOC 2 Type II compliance and can provide its audit report upon request. Provider maintains compliance with such additional data security frameworks as identified in **Exhibit C**, attached hereto. Provider's security

program is aligned with the NIST Cybersecurity Framework and CIS Controls. Provider will implement and maintain reasonable technical and organizational security measures, policies, and procedures, including physical access control, backup, and encryption (where such encryption satisfies guidance promulgated by the U.S. Department of Health and Human Services), to protect the Student Data. Provider shall provide, upon request, contact information of an employee who the LEA may contact if there are any data security concerns or questions.

6.4 **Data Breach.** 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. In the event of a Data Breach originating from the LEA's use of the Service or otherwise a result of LEA's actions or inactions, Provider shall reasonably cooperate with the LEA to the extent necessary to expeditiously secure Student Data and may request costs incurred as a result of such Data Breach.

a) **Notice.** In the event of a Data Breach, the Provider shall provide notice to the LEA's designated representative without undue delay, but not longer than seventy-two (72) hours after confirmation of the Data Breach, so that notification can occur as required by applicable state law. Provider may delay notice if requested to do so by law enforcement. The notice shall include the following information, to the extent known: (a) a description of the Data Breach in general terms; (b) the type of Student Data that was subject to unauthorized release, disclosure, or acquisition; (c) identification of impacted individuals, if known; (d) whether notification was delayed at the request of law enforcement; and (e) the date or estimated date of the Data Breach. The LEA shall provide notice and facts surrounding the Data Breach to the affected students, parents, or legal guardians.

b) **Incident Response Plan.** Provider further acknowledges and agrees to have a written incident response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach and agrees to provide the LEA, upon request, with a summary of said written incident response plan

6.5 **Unique Identifiers.** Where legally required, Provider shall (1) use a unique identifier established by the LEA for any account creation, data upload, data transmission, analysis, or reporting to mask personally identifiable information of students; and (2) adhere to a state-required student data sharing agreement that includes an established unique identifier standard for all operators as prescribed by the agency.

7. MISCELLANEOUS

7.1 **Termination.** This DSA shall stay in effect for the duration of the Term as defined in the Terms.

7.2 **Entire Agreement.** This DSA 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. 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.

- 7.3 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. 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 DSA or affecting the validity or enforceability of such provision in any other jurisdiction.
- 7.4 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. 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.
- 7.5 Notices.** All notices under this DSA shall be in writing and shall be deemed to have been duly given when received, if personally delivered or sent by certified or registered mail, return receipt requested; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; or the day after it is sent, if sent for next day delivery by recognized overnight delivery service. Notices must be sent to the contacts for each Party set forth on the PO (as defined in the Terms) or other ordering document. Either Party may update its address set forth above by giving notice in accordance with this section.

EXHIBIT A: OVERVIEW OF PROVIDER SERVICES

DESCRIPTION OF SERVICES	• Provider offers the following products: ○ Amira Tutor, 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, a suite of 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. • Provider’s products support core instruction and early identification of reading difficulties, including indicators of dyslexia, and provide actionable data for targeted instruction. • Provider offers teacher and staff training, implementation support, and access to student-level data and reporting tools.		
CATEGORIES OF STUDENT DATA COLLECTED	<table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top; width: 50%;"> Application Technology Metadata • IP addresses of users, use of cookies, etc. • Other application technology metadata: 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 • Other enrollment information: class enrollment Schedule • Teacher names (collected for rostering and reporting purposes; not Student Data under this DSA) </td><td style="vertical-align: top; width: 50%;"> Student Identifiers • Local (school district) ID number • State-assigned student ID number • Provider/app-assigned student ID number • Student app username 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) • Audio Data – The Services process recordings of students reading aloud (“Audio Data”) solely to provide real-time instructional feedback and assess reading accuracy, fluency, and comprehension. Amira does not use Audio Data for identification, authentication, speaker recognition, or surveillance, and does not create or store voiceprints, voice templates, or similar representations of vocal characteristics for those purposes. Any use of Audio Data for product improvement is de-identified. Audio Data is subject to Section 5.3’s retention and disposition requirements. </td></tr> </table>	Application Technology Metadata • IP addresses of users, use of cookies, etc. • Other application technology metadata: 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 • Other enrollment information: class enrollment Schedule • Teacher names (collected for rostering and reporting purposes; not Student Data under this DSA)	Student Identifiers • Local (school district) ID number • State-assigned student ID number • Provider/app-assigned student ID number • Student app username 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) • Audio Data – The Services process recordings of students reading aloud (“Audio Data”) solely to provide real-time instructional feedback and assess reading accuracy, fluency, and comprehension. Amira does not use Audio Data for identification, authentication, speaker recognition, or surveillance, and does not create or store voiceprints, voice templates, or similar representations of vocal characteristics for those purposes. Any use of Audio Data for product improvement is de-identified. Audio Data is subject to Section 5.3’s retention and disposition requirements.
Application Technology Metadata • IP addresses of users, use of cookies, etc. • Other application technology metadata: 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 • Other enrollment information: class enrollment Schedule • Teacher names (collected for rostering and reporting purposes; not Student Data under this DSA)	Student Identifiers • Local (school district) ID number • State-assigned student ID number • Provider/app-assigned student ID number • Student app username 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) • Audio Data – The Services process recordings of students reading aloud (“Audio Data”) solely to provide real-time instructional feedback and assess reading accuracy, fluency, and comprehension. Amira does not use Audio Data for identification, authentication, speaker recognition, or surveillance, and does not create or store voiceprints, voice templates, or similar representations of vocal characteristics for those purposes. Any use of Audio Data for product improvement is de-identified. Audio Data is subject to Section 5.3’s retention and disposition requirements.		

EXHIBIT B

DIRECTIVE FOR DISPOSITION OF DATA

LEA directs Provider to dispose of data obtained by Provider 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 to the following site as follows:
[Insert or attach special instructions]

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 C

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:

- **National Institute of Standards and Technology (NIST CSF 2.0):** Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF)
- **American Institute of Certified Public Accountants (AICPA):** Systems and Organization Controls (SOC 2)
- **Center for Internet Security (CIS):** CIS Controls

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 on www.amiralearning.com.