STANDARD HAWAII DATA SHARE AGREEMENT

HI-DSA Standard
Version *2.0*
(7.16.24)

(SCHOOL / COMPLEX AREA / STATE)

and

Amplify Education, Inc.

(COMPANY / VENDOR NAME)

This Agreement Expires on: _____
(DSA Expiration Date)

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

_____ (the "Department") located at:
(School/Complex Area/State)

_____
(School/Complex Area/State Address)

and Amplify Education, Inc. (the "Provider"), located at:
(Company/Vendor Name)

55 Washington Street, Suite 800, Brooklyn, NY 11201.
(Company/Vendor Business Address)

WHEREAS, the Provider is providing educational or digital services to the Department pursuant to the Price Quotes which incorporate the Provider's terms and conditions located at https://amplify.com/customer-terms (the "Services Agreement").

WHEREAS, the Provider and Department 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); Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h, Health Insurance Portability and Accountability Act of 1996 at 45 C.F.R. Part 160, Part 162, and Part 164 ("HIPAA"); and applicable state privacy laws and regulations, such as Hawaii Revised Statutes ("HRS") 487N Security Breach of Personal Information, HRS. 487G, Uniform Employee and Student Online Privacy Protection Act, and Hawaii Administrative Rules ("HAR") 8-34, Protection of Educational Rights and Privacy of Students and Parents; and

WHEREAS, the Provider and Department 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, Department and Provider agree as follows:

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

2. 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 of Service or Privacy Policy the terms of this DSA shall control.

3. This DSA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DSA was signed.

4. The services to be provided by Provider to Department 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 **Department** for this DSA is:

Name: _____ Title: _____

Phone: _____ Email: _____

The designated representative for the **Provider** for this DSA is:

Name: Aaron Harnly Title: CTO

Phone: (800) 823-1969 Email: privacy@amplify.com

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

DEPARTMENT: _____
(School/Complex Area/State)

BY: _____ Date: _____
(Department Signature)

Printed Name: _____ Title/Position: _____

PROVIDER: Amplify Education, Inc.
(Provider/Company Name)

BY: Catherine MacKay Date: 08 / 05 / 2024
(Provider Signature)

Printed Name: Catherine Mackay Title/Position: President & COO

_____
Reviewed by DGA

STANDARD CLAUSES
Version 1

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 these services, the Provider shall be considered a Department Official with a legitimate educational interest, and performing services otherwise provided by the Department. Provider shall be under the direct control and supervision of the Department, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, Department shall provide Student Data as identified in the Schedule of 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 Department**. 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 Department. 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 that contain Student Data, 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 Department. For the purposes of FERPA, the Provider shall be considered a Department Official, under the control and direction of the Department as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the Department 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 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 a Department to respond to a parent or student, whichever is sooner) to the Department'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 Department, 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 Department, transfer, or provide a mechanism for the Department 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 Department in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Department of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the
Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DSA.

ARTICLE III: DUTIES OF DEPARTMENT

1. **Provide Data in Compliance with Applicable Laws**. Department 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 Department has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), Department shall include a specification of criteria for determining who constitutes a "Department official" and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. Department shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data. If appropriate, the Department will obtain consent forms.

4. **Unauthorized Access Notification**. Department shall notify Provider promptly of any known unauthorized access. Department 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 Hawaii and Federal law and regulations pertaining to data privacy and security, 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), Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h, Health Insurance Portability and Accountability Act of 1996 at 45 C.F.R. Part 160, Part 162, and Part 164("HIPAA"), and applicable state privacy laws and regulations, such as Hawaii Revised Statutes ("HRS") 487N Security Breach of Personal Information, HRS 487G, Uniform Employee and Student Online Privacy Protection Act, and Hawaii Administrative Rules ("HAR") 8-34, Protection of Educational Rights and Privacy of Students and Parents; 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**" or 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 confidentiality obligations no less stringent than 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 necessary to provide the services under the Services Agreement or as directed or permitted by the Department 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 Department or other governmental agencies in conducting research and other studies; and (2) research, development, or improvement of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for other legitimate educational purposes,adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DSA or any request by Department to return or destroy Student Data. Except for subprocessors, Provider agrees not to transfer de- identified Student Data to any

party unless that party agrees in writing not to attempt re-identification. Prior to publishing any document that names the Department explicitly, the Provider shall obtain the Department's written approval of the manner in which De-Identified data is presented.

6. **Disposition of Data**. Upon written request from the Department, Provider shall dispose of or provide a mechanism for the Department to transfer Student Data obtained under the Service Agreement, within ninety (90) 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 Department is received, Provider shall dispose of all Student Data after providing the Department 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 section II 3. The Department may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the Department 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.

7. **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 Service to Department. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or Department 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; provided that technical personnel may access software applications containing Student Data for the purpose of providing customer support. Upon request of the Department, 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 Department with at least thirty (30) days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the Department 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 services to the Department. The Provider will cooperate reasonably with the Department 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 Department, and shall provide reasonable access to the Provider's facilities, staff, agents and Department's Student Data and all records pertaining to the Provider, Department and delivery of Services to the Department. Failure to reasonably cooperate shall be deemed a material breach of the DSA. Notwithstanding the foregoing, Provider will only permit such audits to the extent required by applicable law. Further, as a vendor to multiple state and district customers, Provider cannot allow direct access to its

systems. Upon request, Provider will provide LEA with results of the most recent third party security assessment report that is relevant to LEA's data.

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 "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DSA, contact information of an employee who Department may contact if there are any data security concerns or questions. Policies and other information of the type described in this section shall be deemed Confidential Information of Provider. If a public records request is made by a third party for Provider's Confidential Information, consistent with applicable law, LEA will give Provider notice of receipt of the request prior to compliance to enable Provider to take protective action it may deem appropriate to attempt to prevent disclosure of such Confidential Information.

   Data Breach. Provider's breach notification obligations will be governed by Exhibit "F", attached hereto and applicable law.

ARTICLE VI: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DSA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DSA and any Service Agreement or contract if the other party breaches any terms of this DSA and fails to cure such breach within thirty (30) days of receipt of notice of such breach..

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of Department's Student Data pursuant to Article IV, section 6.

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. 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. This Agreement supersedes any other prior agreement or understandings reached by the Parties regarding the matters set forth herein, and any amendments to the terms of this Agreement shall not be binding, unless they are set forth in writing and signed by authorized representatives of the 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 DocuSign shall be considered an "original" signature page for purposes of this Agreement. The submission of a signature page transmitted by facsimile, PDF format (via e- mail), or other similar electronic transmission facility, shall be considered an "original" signature page for purposes of this Agreement so long as the original signature page is thereafter transmitted by mail or by other delivery service.

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. 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. **Governing Law; Venue and Jurisdiction**. THIS DSA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF HAWAII, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE Department 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 Department 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 Department 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. Such approval shall not be unreasonably withheld.

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.

Remainder of this page intentionally left blank.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Amplify Education Inc. ("Amplify") provides core curriculum and supplemental programs and services in ELA, math, and science, and formative assessment products in early reading and math.

The selected items in Exhibit B list all categories of data which may be collected from Amplify's products. If you have questions about which data elements are collected for your LEA's selected products, please contact privacy@amplify.com.

Amplify uses Student Data collected from, or on behalf of, an LEA to support the learning experience, to provide Amplify products to the LEA and to ensure secure and effective operation of our products, including: to provide and improve our educational products and to support LEAs' and authorized users' activities; for purposes requested or authorized by the LEA or as otherwise permitted by applicable laws; for adaptive or personalized learning purposes, provided that Student Data is not disclosed; for customer support purposes, to respond to the inquiries and fulfill the requests of LEAs and their authorized users; to enforce product access and security controls; and to conduct system audits and improve protections against the misuse of our products, or to detect and prevent fraud and other harmful activities.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System	
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☑	
	Other application technology meta data. Please specify: Browser User Agent; Operating system brand and version; Browser brand and version	☑	
Application Use Statistics	Meta data on user interaction with application	☑	
Assessment	Standardized test scores	☐	
	Observation data	☑	optional
	Other assessment data. Please specify: Optional interim and unit assessments	☑	optional
Attendance	Student school (daily) attendance data	☐	
	Student class attendance data	☐	
Communications	Online communications captured (emails, blog entries)	☐	
Conduct	Conduct or behavioral data	☐	
Demographics	Date of Birth	☑	If students are rostered: Optional
	Place of Birth	☐	
	Gender	☑	optional
	Ethnicity or race	☑	optional
	Language information (native, or primary language spoken by student)	☑	optional
	Other demographic information. Please specify: Additional CEDS-aligned demographics may be optionally suppload for aggregate reporting purposes	☑	optional
Enrollment	Student school enrollment	☑	
	Student grade level	☑	
	Homeroom	☑	optional
	Guidance counselor	☐	

	Specific curriculum programs	✔	
	Year of graduation	☐	
	Other enrollment information. Please specify:	☐	
Parent/Guardian Contact Information	Address	☐	
	Email	☐	
	Phone	☐	
Parent/Guardian ID	Parent ID number (created to link parents to students)	☐	
Parent/Guardian Name	First and/or Last	☐	
Schedule	Student scheduled courses	✔	
	Teacher names	✔	
Special Indicator	English language learner information	✔	optional
	Low income status	✔	optional
	Medical alerts/health data	☐	
	Student disability information	✔	optional
	Specialized education services (IEP or 504)	✔	optional
	Living situations (homeless/foster care)	☐	
	Other indicator information. Please specify: Additional CEDS- aligned demographic indicators may be optionally supplied for aggregate reporting purposes	✔	optional
Student Contact Information	Address	☐	
	Email	✔	
	Phone	☐	
Student Identifiers	Local (School district) ID number	✔	
	Student ID number	✔	optional
	Provider/App assigned student ID number	☐	
	Student app username	✔	optional
	Student app passwords	✔	optional
	Student password hint	☐	
Student Name	First and/or Last	✔	

Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	☑
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☑
Student work	Student generated content; writing, pictures, etc.	☑
	Other student work data. Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/ performance scores	☐
	Other transcript data. Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

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 reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the Department or local education agency, or by a person acting for such Department or local education agency, 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.

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 have been stripped of all direct and indirect identifiers are 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 Department purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with a school(s) to provide a service to that Department shall be considered an "operator" for the purposes of this section.

Originating School: A School who originally executes the DSA in its entirety with the Provider.

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. Within the DSA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

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.

Department Official: For the purposes of this DSA and pursuant to 34 CFR § 99.31(b), a Department 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 CFR § 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 refers to personally identifiable information (PII) of students in any data, whether gathered by Provider or provided by Department or its users, students, or students' parents/guardians. PII means information that, alone or in combination with other information, can be used to identify a person with reasonable certainty 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 Meta Data. 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.

Subprocessor: For the purposes of this DSA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Department 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.

Subscribing School: A school that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

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.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud- based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DSA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

_____: Provider to dispose of data obtained by Provider
(School Name/Complex Area/State)

pursuant to the terms of the Service Agreement between Department 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 of deletion of data.

☐ Disposition shall be by transfer of data. The data shall be transferred to the following site as follows: [Insert of attach special instructions]

3. Schedule of Disposition

Data will be disposed of by the following date:

☐ As soon as commercially practicable

☐ By: _____

(Date)

4. Signature

_____ _____

Authorized Representative of School Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks 2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	**FRAMEWORK(S)**
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

Exhibit “F”

Security Incident

1. Data Security Incident. If Amplify Education Inc. (“Amplify”) has reason to believe that Student Data are disclosed to or acquired by an unauthorized individual(s) (a “Security Incident”), then Amplify will fully investigate the incident and to take reasonable steps to remediate systems and controls and to mitigate any potential harm to individuals which may result from the Security Incident and cooperate with LEA’s investigation of the Security Incident.

2. Notification to District. Amplify will notify LEA after Amplify determines that LEA’s Student Data were affected by the Security Incident, subject to applicable law and authorization of law enforcement personnel, if applicable. Notification to the LEA will occur as soon as practical and within seven (7) days of determination that the LEA’’s Student Data were affected by the Security Incident. To the extent known, Amplify will identify in such a notification the following: (i) the nature of the Security Incident, (ii) the steps Amplify has executed to investigate the Security Incident, (iii) the type(s) of personally identifiable information that was subject to the unauthorized disclosure or acquisition, (iv) the cause of the Security Incident, if known, (v) the actions Amplify has done or will do to remediate any deleterious effect of the Security Incident, and (vi) the corrective action Amplify has taken or will take to prevent a future Security Incident.

3. Notification to Individuals. To the extent LEA determines that the Security Incident triggers third party notice requirements under applicable laws, as the owner of the Student Data, the LEA shall be responsible for the timing and content of the notices to be sent. Except as otherwise required by law, Amplify will not provide notice of the Security Incident directly to individuals whose personal information was affected, to regulatory agencies, or to other entities, without first providing written notice to the LEA. Amplify will be responsible for, and will bear, all notification related costs arising out of or in connection with the Security Incident, subject to any limitations of liability terms contained in the Agreement. For clarity and without limitation, Amplify will not be responsible for costs associated with voluntary notification that is not legally required. With respect to any Security Incident that is not due to acts or omissions of Amplify or its agents, Amplify will reasonably cooperate in performing the activities described above, at LEA’s reasonable request and expense.