OK AS TO FORM AMH 2-28-2025

AMENDMENT TO THE DATA PRIVACY AGREEMENT BETWEEN AMPLIFY EDUCATION, INC. AND JEFFERSON COUNTY BOARD OF EDUCATION

THIS AMENDMENT TO THE CONTRACT BETWEEN Amplify Education Inc, AND JEFFERSON COUNTY BOARD OF EDUCATION (hereinafter "Amendment") is entered by and between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools (hereinafter "JCPS") with its principal place of business located at 3332 Newburg Road, Louisville, Kentucky 40218, and, Amplify Education Inc (hereinafter "Provider") with its principal place of business located at 55 Washington Street, Suite 800, Brooklyn, NY 11201.

WHEREAS, The Parties have entered into a Data Privacy Agreement for the procurement of educational or digital services to the Board effective July 26, 2023 (the "Agreement"); and

WHEREAS, The Parties wish to alter the agreement.

THEREFORE, the Parties wish to amend the Exhibit A and Exhibit B of the agreement between Amplify Education Inc and JCPS Board of Education.

This Amendment hereby amends Exhibit A as follows to add the following:

DESCRIPTION OF SERVICES
The following is hereby added to the Description of Services:

Amplify Fluency – online digital tool available for all schools

The following is hereby added to the Compensation for Amplify Fluency:

Funds for purchase shall come individual school or department budgets. ~~from account code CM12293-0349-473GL~~. Total payments under this DPA shall not typical vendor pricing per fiscal year, running from July I-June 30.

The attached Exhibit B is hereby added to the Agreement as a supplement to the existing Exhibit B.

All other provisions of the Agreement shall remain unchanged. This Amendment is the entire agreement of the parties regarding modifications of the Agreement provided herein, supersedes all prior agreements and understandings regarding such subject matter, may be modified only by a writing executed by the parties. The Agreement is ratified and confirmed in full force and effect in accordance with its terms, as amended hereby. In the

event of any conflict between the terms of the Agreement and this Amendment, the provisions of this Amendment shall control.

This Amendment may be executed via electronic signature in one of more counterparts, each of which will be deemed an original, but all such electronic signatures and counterparts will together constitute but one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment to be effective as of April 9, 2025.

Jefferson County Public Schools:

By: _____

Dr. Martin A. Pollio

Superintendent

Date: _____

Amplify Education Inc.

By: _____

Jason Zimba (Mar 17, 2025 11:04 EDT)

Jason Zimba

EVP and CAO, Math

Date: Mar 17, 2025

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check If Used by Your System (Windows)	Check If Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check If Used by Your System (iOS)	Check If Used by Your System (Browser Based)	Check If Used by Your System (Other, please specify: _____)
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	☐	☐	☐	☑	☐
	Other assessment data-Please specify: Optional interim and unit assessments	☐	☐	☐	☑	☐
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	☐	☐	☐	☐	☐
	Place of Birth	☐	☐	☐	☐	☐
	Gender Note: Optional	☐	☐	☐	☑	☐
	Ethnicity or race Note: Optional	☐	☐	☐	☑	☐
	Language information (native, or primary language spoken by student) Note: Optional	☐	☐	☐	☑	☐
	Student disability information	☐	☐	☐	☐	☐

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (iOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Other demographic information-Please specify:	☐	☐	☐	☐	☐
Enrollment	Student school enrollment	☐	☐	☐	☑	☐
	Student grade level	☐	☐	☐	☑	☐
	Homeroom	☐	☐	☐	☐	☐
	Guidance counselor	☐	☐	☐	☐	☐
	Specific curriculum programs	☐	☐	☐	☐	☐
	Year of graduation	☐	☐	☐	☐	☐
	Other enrollment information-Please specify: Additional CEDS-aligned demographics may be optionally supplied for aggregate reporting purposes	☐	☐	☐	☑	☐
Parent/Guardia n 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	☐	☐	☐	☐	☐
	Low income status	☐	☐	☐	☐	☐
	Medical alerts/ health data	☐	☐	☐	☐	☐

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (iOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Specialized education services (IEP or 504)	☐	☐	☐	☐	☐
	Living situations (homeless/foster care)	☐	☐	☐	☐	☐
	Other indicator information-Please specify:	☐	☐	☐	☐	☐
Staff Data	First and Last Name	☐	☐	☐	☑	☐
	Email Address	☐	☐	☐	☑	☐
	Staff ID number	☐	☐	☐	☑	☐
	Other information – Please specify	☐	☐	☐	☐	☐
Student Contact Information	Address	☐	☐	☐	☐	☐
	Email	☐	☐	☐	☑	☐
	Phone	☐	☐	☐	☐	☐
Student Identifiers	Local (School district) ID number	☐	☐	☐	☑	☐
	State ID number Note: Optional	☐	☐	☐	☑	☐
	Provider/App assigned student ID number	☐	☐	☐	☐	☐
	Student app username Note: Optional. SSO is recommended	☐	☐	☐	☑	☐
	Student app passwords Note: Optional. SSO is recommended.	☐	☐	☐	☑	☐
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.	☐	☐	☐	☑	☐

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (iOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Other student work data -Please specify:	☐	☐	☐	☐	☐
Transcript	Student course grades	☐	☐	☐	☐	☐
	Student course data	☐	☐	☐	☐	☐
	Student course grades/ performance scores	☐	☐	☐	☑	☐
	Other transcript data - Please specify:	☐	☐	☐	☐	☐
Transportation	Student bus assignment	☐	☐	☐	☐	☐
	Student pick up and/or drop off location	☐	☐	☐	☐	☐
	Student bus card ID number	☐	☐	☐	☐	☐
	Other transportation data – Please specify:	☐	☐	☐	☐	☐
Other	Please list each additional data element used, stored, or collected by your application:	☐	☐	☐	☐	☐
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	☐	☐	☐	☐	☐

JEFFERSON COUNTY BOARD OF EDUCATION

July 25, 2023

Agenda Item: **VII.N.15. Recommendation for Approval of Data Privacy Agreement with Amplify Education Inc. for the 2023-24 and 2024-25 School Years**

Recommendation: Superintendent Martin Pollio recommends the Board of Education approve the attached Data Privacy Agreement with Amplify Education Inc. and authorize the superintendent sign same.

Rationale: Amplify Education Inc. for science is rooted in the Lawrence Hall of Science's Do, Talk, Read, Write, Visualize model of learning and was designed to align with the Next Generation Science Standards. With the multimodal approach (Do, Talk, Read, Write, Visualize), students have multiple pathways through which to access content and demonstrate their understanding of standards and key concepts which promotes equity and engagement.

Gold standard research shows that this pedagogical approach improves outcomes in literacy and science for all students. Amplify Education Inc. meets the criteria for Tier III-Promising Evidence as an education
intervention under ESSA.

Submitted by Dr. Terra Greenwell

Attachment

OK AS TO FORM
A.M.H. 10.26.2023

This Confidential Data Privacy Agreement ("**DPA**") is entered into by and between:

THE BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY, a political subdivision of the Commonwealth of Kentucky, with its principal place of business at 3332 Newburg Road, Louisville, Kentucky 40218 (the "**Board**" or "**Jefferson County Public Schools**") and

Amplify Education, Inc., a corporation organized under the laws of Delaware with its principal place of business located at 55 Washington Street, Suite 800, Brooklyn, NY 11201 (the "**Provider**" or "Amplify").

WHEREAS, the Provider is providing educational or digital services to the Board.

WHEREAS, the Provider and the Board 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 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and the Board desire to enter into this DPA 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 Board and Provider agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Entire Agreement.** Regarding the subject matter contemplated hereunder, this DPA is the entire agreement between the Parties and supersedes any and all agreements, representations, and negotiations, either oral or written, between the Parties before the effective date of this DPA. This DPA may not be amended or modified except in writing as provided below. This DPA is supplemented by the Board's Procurement Regulations currently in effect (hereinafter "Regulations"), and Amplify's Customer Terms and Conditions and Privacy Policy, attached hereto as Exhibit "G", that are incorporated by reference into and made part of this DPA. In the event of a conflict between any provision of this DPA and the Regulations or Exhibit G, the Regulations shall prevail, and the DPA shall prevail over Exhibit G to the extent of any conflict. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

2. **Term.** This DPA shall be effective as of July 26, 2023 (the "**Effective Date**") and shall continue for three (3) years, terminating on July 25, 2026.

3. **Services.** The services to be provided by Provider to the Board pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**"). Any compensation to be provided by the Board to Provider is also detailed in **Exhibit "A"** (the "**Compensation**"). Each party shall be responsible for their portion of costs that may result from data sharing that is required by law or otherwise agreed to between the parties. Examples of potential costs to the Board are costs associated with the compiling of Confidential Data requested under this DPA and costs associated with the electronic delivery of Confidential DATA to Provider.

4. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Confidential 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, and performing services otherwise provided by the Board. Provider shall be under the direct control and supervision of the Board, with respect to its use of Confidential Data.

5. **Confidential Data to Be Provided.** In order to perform the Services described above, the Board shall provide Confidential Data as identified in the Schedule of Data, attached hereto as **Exhibit "B".**

6. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in 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. **Confidential Data Property of the Board.** All Confidential 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 Board. The Provider further acknowledges and agrees that all copies of such Confidential Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, to the extent such modifications additions or portions contain Confidential Data, are subject to the provisions of this DPA in the same manner as the original Confidential Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Confidential Data contemplated per the Service Agreement, shall remain the exclusive property of the Board. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Board as it pertains to the use of Confidential Data, notwithstanding the above.

2. **Parent Access.** To the extent required by law the Board shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Confidential 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 the Board to respond to a parent or student, whichever is sooner) to the Board's request for Confidential 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 Confidential Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Board, 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 Board, transfer, or provide a mechanism for the Board 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 Confidential Data held by the Provider pursuant to the Services, the Provider shall notify the Board in advance of a compelled

disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board 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 Confidential Data in a manner no less stringent than the terms of this DPA.

6. **Research and Program Evaluation.** For any project, involving data collection or research (e.g., program evaluation or monitoring activities), student or staff participation is voluntary. As a federally authorized Institutional Review Board (IRB), the Board complies with the federal definition for research, which includes sharing of Personally Identifiable Information (PII) for the purposes of answering a question or evaluating activities for effectiveness beyond standard educational or operational procedures. Thus, all data collection and research activities must be approved by the Board's IRB and shall not begin before approval is secured from the IRB. If Provider wishes to collect data specifically for program evaluation or research purposes, or if Provider wishes to use identifiable data for program evaluation or research purposes, Provider must apply for and obtain permission from the Board's IRB prior to beginning any research or evaluation related data collection.

ARTICLE III: DUTIES OF THE BOARD

1. **Provide Data in Compliance with Applicable Laws.** The Board shall provide Confidential 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 Board has a policy of disclosing Education Records and/or Confidential Data under FERPA (34 CFR § 99.31(a)(1)), the Board 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 Board shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Confidential Data.

4. **Unauthorized Access Notification.** The Board shall notify Provider promptly of any known unauthorized access. The Board 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, state, and local laws, rules, and regulations pertaining to Confidential Data privacy and security, all as may be amended from time to time, including but not limited to FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.

2. **Data Custodian.** For the purposes of this DPA and ensuring Provider's compliance with the terms of this DPA and all application of state and federal law, Provider designated Aaron Harnly, CTOas the data custodian ("Data Custodian") of the Confidential Data. The Board will release all data and information under this DPA to Data Custodian. Data Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this DPA, including confirmation of the return or destruction of data as described below. The Board may, upon request, review the records Provider is required to keep under this DPA.

3. **Authorized Use.** The Confidential 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 DPA. Provider will not contact the individuals included in the data sets without obtaining advance written authorization from the Board.

4. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Confidential Data to comply with obligations no less stringent than those of the applicable provisions of this DPA with respect to the Confidential Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Confidential Data pursuant to the Service Agreement.

5. **Insurance.** Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of $5M. Upon request, Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

Board of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville, Kentucky 40218

6. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Confidential Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Confidential Data other than as necessary to provide the Services or as required by law or court order. If Provider becomes legally compelled to disclose any Confidential Data (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), then Provider shall use all reasonable efforts to provide the Board with prior notice before disclosure so that the Board may seek a protective order or other appropriate remedy to present the disclosure or to ensure the Board's compliance with the confidentiality requirements of federal or state law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Confidential Data to any third party.

7. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Confidential Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Board or other governmental agencies in conducting research and other studies; and (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 purpose and for customized student Learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by the Board to return or destroy Confidential Data. Except for Subprocessors, Provider agrees not to transfer de-identified Confidential Data to any party unless (a) that party agrees in writing not to attempt re-identification. Prior to publishing any document that names the Board explicitly or indirectly, the Provider shall obtain the Board's prior written approval.

8. **Disposition of Data.** Upon written request from the Board, Provider shall dispose of or provide a mechanism for the Board to transfer Confidential Data obtained under the Service Agreement in a usable format, 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 DPA without a subsequent agreement in place, if no written request from the Board is received to return the data in a usable format, Provider shall dispose of all Confidential Data in accordance with Provider's data retention and deletion policies. The duty to dispose of Confidential Data shall not extend to Confidential Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The JCPS may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the JCPS and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Confidential Data described in **Exhibit "D"**.

9. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Confidential 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 the Board. This section does not prohibit Provider from using Confidential Data (i) for adaptive Learning or customized student Learning (including generating personalized Learning recommendations); or (ii) to make product recommendations to teachers or JCPS employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Confidential Data as permitted in this DPA and its accompanying exhibits.

10. **Liability.** Provider agrees to be responsible for and assumes all liability for any claims, costs, damages or expenses (including reasonable attorneys' fees) that may arise from or relate to Provider's intentional or negligent release of personally identifiable student, parent or staff data ("Claim" or "Claims"). Provider agrees to hold harmless the Board and pay any costs incurred by the Board in connection with any Claim. The provisions of this Section shall survive the termination or expiration of this DPA.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Confidential Data shall be stored within the United States. Upon request of the Board, Provider will provide a list of the locations where Confidential Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the Board with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the Board to audit the security and privacy measures that are in place to ensure protection of Confidential Data or any portion thereof as it pertains to the delivery of services to the JCPS . The Provider will cooperate reasonably with the Board 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 Board, and shall provide reasonable access to the Provider's facilities, staff, agents and the Board's Confidential Data and all records pertaining to the Provider, the Board and delivery of Services to the Board. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Confidential 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 standards set forth in **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, in the Standard Schedule to the DPA, contact information of an employee who the Board may contact if there are any data security concerns or questions. Additionally, The Provider agrees to maintain a minimum security standard including but limited to the following precautions and protections:

    a) Encrypting all data, at rest and in transit;
    b) Maintaining multi-factor authentication on accounts that can access the network or email remotely, including 3rd party accounts;
    c) Establishing and enforcing well-defined data privilege rights which follow the rule of least privilege and restrict users' access to the data necessary for this to perform their job functions;
    d) Ensuring all staff and 3rd parties are bound by confidentiality obligations no less stringent those of this DPA;

4. **Data Breach.** Provider's Data Breach obligations will be governed by Exhibit F, attached hereto.

5. **Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act.** If Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:

    a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

        i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;

        ii. A Social Security number;

        iii. A taxpayer identification number that incorporates a Social Security number;

iv. A driver's license number, state identification card number or other individual identification number issued by an agency;

v. A passport number or other identification number issued by the United States government; or

vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.

c. Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.

d. Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

e. Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

6. **Cloud Computing Service Providers.** If Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Provider agrees that:

Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

Pursuant to KRS 365.734(2), Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

Pursuant to KRS 365.734(2), Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.

Pursuant to KRS 365.734(3), Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).

ARTICLE VI: MISCELLANEOUS

7. **Termination.** Either party may terminate this DPA if the other party breaches any terms of this DPA, provided however, the breaching party shall have thirty (30) days to cure such breach and this DPA shall remain in force. The Board may terminate this DPA in whole or in part at any

time by giving written notice to Provider of such termination and specifying the effective data thereof, at Least thirty (30) days before the specified effective data. In accordance with **Attachment A,** the Board shall compensate Provider for Services satisfactorily performed through the effective date of termination.

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

9. **Priority of Agreements.** This DPA shall govern the treatment of Confidential Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence.

10. **Modification.** No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

11. **Disputes.** Any differences or disagreements arising between the Parties concerning the rights or liabilities under this DPA, or any modifying instrument entered into pursuant to this DPA, shall be resolved through the procedures set out in the Regulations.

12. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or certified mail, sent to the designated representatives below.

The designated representative for the Board for this DPA is:

Name: Dr. Terra Greenwell Title: Chief Academic Officer

Address: 3332 Newburg Road, Louisville, KY 40213

Phone: 502-485-3011 Email: terra.greenwell@jefferson.kyschools.us

The designated representative for the Provider for this DPA is:

Name: Aaron Harnly Title: CTO
Address: 55 Washington Street, Suite 800, Brooklyn, NY 11201

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

13. **Amendment and Waiver.** This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

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

15. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE COMMONWEALTH OF KENTUCKY, 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 JEFFERSON COUNTY KENTUCKY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

16. **Successors Bound:** This DPA 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 DPA, the Provider shall provide written notice to the Board 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 DPA and any obligations with respect to Confidential Data within the Service Agreement. The Board has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

17. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Confidential Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Confidential Data and/or any portion thereof.

18. **Relationship of Parties.** The Board is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor the Board shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

19. **Equal Opportunity.** During the performance of this DPA, Provider agrees that Provider shall not discriminate against any employee, applicant or subcontractor because of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex, sexual orientation, gender identity, gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions. If the Compensation is paid from federal funds, this DPA is subject to Executive Order 11246 of September 24, 1965 and in such event the Equal Opportunity Clause set forth in 41 Code of Federal Regulations 60-1.4 is hereby incorporated by reference into this DPA as if set forth in full herein.

20. **Prohibition on Conflicts of Interest.** It shall be a breach of this DPA for Provider to commit any act which is a violation of Article XI of the Regulations entitled "Ethics and Standards of Conduct," or to assist or participate in or knowingly benefit from any act by any employee of the Board which is a violation of such provisions.

21. Contractor shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342 that apply to Provider for the duration of this DPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.

22. **Access to School Grounds.** No employee or agent of Provider shall access the Board's school grounds on a regularly scheduled or continuing basis for purposes of providing services to students under this DPA.

IN WITNESS WHEREOF, The Board and Provider execute this DPA as of the Effective Date above.

BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: Date: 7/26/23
Printed Name: Dr. Marty Pollio
Title/Position: Superintendent

AMPLIFY EDUCATION, INC.
By: Alexandra Walsh Date: 07 / 06 / 2023
Printed Name: Alexandra Walsh
Title/Position: Chief Product Officer

EXHIBIT "A"

DESCRIPTION OF SERVICES

Provider shall provide software licenses and support for the following products at prices equal or below Provider's standard pricing rates for the products:

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.

Amplify Education, Inc. will provide a combination of in-person (onsite) and virtual (remote) professional learning sessions focused on providing all science teachers in the Elementary Choice zone schools. Throughout the 2023-24 and 2024-25 school year. Professional Learning sessions will include program overview sessions to introduce teachers to the instructional model. digital platform, and instructional resources; unit internalization sessions to prepare teachers for upcoming units of instruction; and strengthening sessions to help teachers prepare to meet the needs of diverse learners in an upcoming lesson. Professional learning for each Choice Zone school will include: a remote program overview session; at least two remote strengthening sessions for the K-5 science teachers, and 1-2 coaching sessions for up to 22 sessions. When needed, additional district-level professional learning sessions will be held for Choice Zone teachers and building leaders to receive additional support and training. Amplify Education, Inc. will have representatives available during the school year to answer any questions or address any concerns that JCPS teachers and/or the JCPS science team might have.

COMPENSATION

Funds for purchase shall come from account code CM12293-0349-473GL. Total payments under this DPA shall not exceed the amounts stated in the applicable purchasing document per fiscal year, running from July 1-June 30.

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	☑
	Other assessment data-Please specify:	☐
Attendance	Student school (daily) attendance data	☐

5.22.23 - AMPLIFY

	Student class attendance data	☐
Communications	Online communications captured (emails, blog entries)	☐
Conduct	Conduct or behavioral data	☐
Demographics	Date of Birth	☑
	Place of Birth	☐
	Gender	☑
	Ethnicity or race	☑
	Language information (native, or primary language spoken by student)	☑
	Student disability information	☑

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify: Additional CEDS-aligned demographics may be optionally supplied for aggregate reporting purposes	☑
Enrollment	Student school enrollment	☑
	Student grade level	☑
	Homeroom	☑
	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	☑
	Low income status	☑
	Medical alerts/ health data	☐

Category of Data	Elements	Check if Used by Your System
	Specialized education services (IEP or 504)	☑
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify: Additional CEDS-aligned demographic indicators may be optionally supplied for aggregate reporting purposes	☑
Staff Data	First and Last Name	☐
	Email Address	☐
	Staff ID number	☐
	Other information – Please specify	☐
Student Contact Information	Address	☐
	Email	☑
	Phone	☐

Student Identifiers	Local (School district) ID number	☑
	State ID number	☑
	Provider/App assigned student ID number	☐
	Student app username	☑
	Student app passwords	☐
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.	☑

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/ performance scores	☐
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐

	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

Compensation: Amounts to be paid to the Provider in exchange for software licenses and support. The maximum amount of Compensation that may be paid under this DPA is set forth in Attachment A. The Board is not obligated to pay the maximum Compensation amount solely by its inclusion in this DPA. Compensation owed is determined by the purchase orders submitted to Provider. The cost for any single license or support provided under this DPA shall not exceed Provider's standard pricing for that product.

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 school or local education agency, or by a person acting for such school 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 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with the Board to provide a service to the Board shall be considered an "operator" for the purposes of this section.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Confidential Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Regulations: The Board Procurement Regulations, available on the JCPS website, as may be amended from time to time.

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.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Confidential 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.

Confidential Data: Confidential Data includes any data, whether gathered by Provider or provided by the Board 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. Confidential Data includes Meta Data. Confidential Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Confidential Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Confidential Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Confidential 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 DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Board 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 Confidential Data.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Confidential 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 Confidential Data, as that term is used in some state statutes. However, for the purpose of this DPA, 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

The Board of Education of Jefferson County Kentucky directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between The Board and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

Signature

_____ _____

Authorized Representative of the Board Date

_____ _____

Verification of Disposition of Data

Authorized Representative of Provider Date

EXHIBIT "E"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Provider will utilize one of the following known and credible cybersecurity frameworks which can protect digital learning ecosystems.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	American Institute of CPAs	SOC2
	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
X	The Board of Education of Jefferson County	Board provided standardized questionnaire

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 District's investigation of the Security Incident.

2. Notification to District. Amplify will notify District after Amplify determines that District's Student Data were affected by the Security Incident, subject to applicable law and authorization of law enforcement personnel, if applicable. 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 District determines that the Security Incident triggers third party notice requirements under applicable laws, as the owner of the Student Data, the District 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 District. 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 District's reasonable request and expense.

Exhibit "G"
CUSTOMER TERMS AND CONDITIONS

1. Scope. Amplify Education, Inc. ("Amplify") and Customer wish to enter into an agreement created by the price quote, proposal, renewal letter, or other ordering document containing the details of this purchase (the "Quote") and these Customer Terms & Conditions, including any addendums hereto (the "Agreement") pursuant to which Amplify will deliver one or more of the products or services specified on the Quote (collectively, the "Products").

2. License. Subject to the terms and conditions of this Agreement, Amplify grants to Customer a non-exclusive, non-transferable, non-sublicenseable license to access and use, and permit Authorized Users, as defined below, to access and use the Products solely in the U.S. for the duration specified in the Quote (the "Term"), for the number of Authorized Users specified in the Quote, for whom Customer has paid the applicable fees to Amplify. "Authorized User" means an individual teacher or other personnel employed by Customer, or an individual student registered for instruction at Customer's school, whom Customer permits to access and use the Products subject to the terms and conditions of this Agreement, and solely while such individual is so employed or so registered. Each Authorized User's access and use of the Products shall be subject to Amplify's Terms of Use available at amplify.com/user-terms and through the Products, in addition to the terms and conditions of this Agreement, and violations of such terms may result in suspension or termination of the applicable account.

3. Restrictions. Customer shall access and use the Products solely for the non-commercial instructional and administrative purposes of Customer's school. Further, Customer shall not, except as expressly authorized or directed by Amplify: (a) copy, modify, translate, distribute, disclose or create derivative works based on the contents of, sell, or otherwise exploit, the Products, or any part thereof; (b) decompile, disassemble, or otherwise reverse engineer the Products or otherwise use the Products to develop functionally similar products or services; (c) modify, alter, or delete any of the copyright, trademark, or other proprietary notices in or on the Products; (d) rent, lease or lend the Products or use the Products for the benefit of any third party; (e) avoid, circumvent or disable any security or digital rights management device, procedure, protocol or mechanism in the Products; or (f) permit any Authorized User or third party to do any of the foregoing. Customer also agrees that any works created in violation of this section are derivative works, and, as such, Customer agrees to assign, and hereby assigns, all right, title and interest in such works to Amplify. The Products and derivatives thereof may be subject to export laws and regulations of the U.S. and other jurisdictions. Customer may not export any Product outside of the U.S. Further, Customer will not permit Authorized Users to access or use any Product in a U.S.-embargoed country or otherwise in violation of any U.S. export law or regulation. The software and associated documentation portions of the Products are "commercial items" (as defined at 48 CFR 2.101), comprising "commercial computer software" and "commercial computer software documentation," as those terms are used in 48 CFR 12.212. Accordingly, if Customer is the U.S. Government or its contractor, Customer will receive only those rights set forth in this Agreement in accordance with 48 CFR 227.7201-227.7204 (for Department of Defense and their contractors) or 48 CFR 12.212 (for other U.S. Government licensees and their contractors).

4. Reservation of Rights. SUBSCRIPTION PRODUCTS ARE LICENSED, NOT SOLD. Subject to the limited rights expressly granted hereunder, all rights, title and interest in and to all Products,

including all related IP Rights, are and shall remain the sole and exclusive property of Amplify or its third-party licensors. "IP Rights" means, collectively, rights under patent, trademark, copyright and trade secret laws, and any other intellectual property or proprietary rights recognized in any country or jurisdiction worldwide. Customer shall promptly notify Amplify of any violation of Amplify's IP Rights in the Products, and shall reasonably assist Amplify as necessary to remedy any such violation. Amplify Products are protected by patents (see amplify.com/virtual-patent-marking).

5. Payments. In consideration of the Products, Customer will pay to Amplify (or other party designated on the Quote) the fees specified in the Quote in full within 30 days of the date of invoice, except as otherwise agreed by the parties or for those amounts that are subject to a good faith dispute of which Customer has notified Amplify in writing. Customer shall be responsible for all state or local sales, use or gross receipts taxes, and federal excise taxes unless Customer provides a then-current tax exemption certificate in advance of the delivery, license, or performance of any Product, as applicable.

6. Shipments. Unless otherwise specified on the Quote, physical Products will be shipped FOB origin in the US (Incoterms 2010 EXW outside of the US) and are deemed accepted by Customer upon receipt. Upon acceptance of such Products, orders are non-refundable, non-returnable, and non-exchangeable, except in the case of defective or missing materials reported to Amplify by Customer within 60 days of receipt.

7. Account Information. For subscription Products, the authentication of Authorized Users is based in part upon information supplied by Customer or Authorized Users, as applicable. Customer will and will cause its Authorized Users to (a) provide accurate information to Amplify or a third-party authentication service as applicable, and promptly report any changes to such information, (b) not share or allow others to use their account, (c) maintain the confidentiality and security of their account information, and (d) use the Products solely via such authorized accounts. Customer agrees to notify Amplify immediately of any unauthorized use of its or its Authorized Users' accounts or related authentication information. Amplify will not be responsible for any losses arising out of the unauthorized use of accounts created by or for Customer and its Authorized Users.

8. Confidentiality. Customer acknowledges that, in connection with this Agreement, Amplify has provided or will provide to Customer and its Authorized Users certain sensitive or proprietary information ("Confidential Information"), including software, source code, assessment instruments, research, designs, methods, processes, customer lists, training materials, product documentation, know-how and/or trade secrets, in whatever form. Customer agrees (a) not to use Confidential Information for any purpose other than use of the Products in accordance with this Agreement and (b) to take all steps reasonably necessary to maintain and protect the Confidential Information of Amplify in strict confidence. Confidential Information shall not include information that, as evidenced by Customer's contemporaneous written records: (i) is or becomes publicly available through no fault of Customer; (ii) is rightfully known to Customer prior to the time of its disclosure; (iii) has been independently developed by Customer without any use of the Confidential Information; or (iv) is subsequently learned from a third party not under any confidentiality obligation.

9. Student Data. The parties acknowledge and agree that in the course of providing the Products to the Customer, Amplify may collect, receive, or generate information that directly relates to an identifiable current or former student of Customer ("Student Data"). Student Data may include personal

information from a student's "educational records," as defined by the Family Educational Rights and Privacy Act of 1974 ("FERPA"). Student Data is owned and controlled by the Customer and Amplify receives Student Data as a "school official" under Section 99.31 of FERPA for the purpose of providing the Products hereunder. Individually and collectively, Amplify and Customer agree to uphold our obligations under FERPA, the Children's Online Privacy Protection Act (COPPA), the Protection of Pupil Rights Amendment (PPRA), and applicable state laws relating to student data privacy. Amplify's Customer Privacy Policy at amplify.com/customer-privacy will govern collection, use, and disclosure of Student Data collected or stored on behalf of Customer under this Agreement.

10. Customer Materials and Requirements. Customer represents, warrants, and covenants that it has all the necessary rights, including consents and IP Rights, in connection with any data, information, content, and other materials provided to or collected by Amplify on behalf of Customer or its Authorized Users using the Products or otherwise in connection with this Agreement ("Customer Materials"), and that Amplify has the right to use such Customer Materials as contemplated hereunder or for any other purposes required by Customer. Customer is solely responsible for the accuracy, integrity, completeness, quality, legality, and safety of such Customer Materials. Customer is responsible for meeting hardware, software, telecommunications, and other requirements listed at amplify.com/customer-requirements.

11. Warranty Disclaimer. PRODUCTS ARE PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND BY AMPLIFY. AMPLIFY EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY AS TO TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR USE. CUSTOMER ASSUMES RESPONSIBILITY FOR SELECTING THE PRODUCTS TO ACHIEVE CUSTOMER'S INTENDED RESULTS AND FOR THE ACCESS AND USE OF THE PRODUCTS, INCLUDING THE RESULTS OBTAINED FROM THE PRODUCTS. WITHOUT LIMITING THE FOREGOING, AMPLIFY MAKES NO WARRANTY THAT THE PRODUCTS WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR WILL MEET CUSTOMER'S REQUIREMENTS. AMPLIFY IS NEITHER RESPONSIBLE NOR LIABLE FOR ANY THIRD PARTY CONTENT OR SOFTWARE INCLUDED IN PRODUCTS, INCLUDING THE ACCURACY, INTEGRITY, COMPLETENESS, QUALITY, LEGALITY, USEFULNESS OR SAFETY OF, OR IP RIGHTS RELATING TO, SUCH THIRD PARTY CONTENT AND SOFTWARE. ANY ACCESS TO OR USE OF SUCH THIRD PARTY CONTENT AND SOFTWARE MAY BE SUBJECT TO THE TERMS AND CONDITIONS AND INFORMATION COLLECTION, USAGE AND DISCLOSURE PRACTICES OF THIRD PARTIES.

12. Limitation of Liability. IN NO EVENT SHALL AMPLIFY BE LIABLE TO CUSTOMER OR TO ANY AUTHORIZED USER FOR ANY INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE OR COVER DAMAGES, DAMAGES FOR LOST PROFITS, LOST DATA OR LOST BUSINESS, OR ANY OTHER INDIRECT DAMAGES, EVEN IF AMPLIFY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, AMPLIFY'S ENTIRE LIABILITY TO CUSTOMER OR ANY AUTHORIZED USER ARISING OUT OF PERFORMANCE OR NONPERFORMANCE BY AMPLIFY OR IN ANY WAY RELATED TO THE SUBJECT MATTER OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE AGGREGATE OF CUSTOMER'S OR

ANY AUTHORIZED USER'S DIRECT DAMAGES UP TO THE FEES PAID BY CUSTOMER TO AMPLIFY FOR THE AFFECTED PORTION OF THE PRODUCTS IN THE PRIOR 12-MONTH PERIOD. UNDER NO CIRCUMSTANCES SHALL AMPLIFY BE LIABLE FOR ANY CONSEQUENCES OF ANY UNAUTHORIZED USE OF THE PRODUCTS THAT VIOLATES THIS AGREEMENT OR ANY APPLICABLE LAW OR REGULATION.

13. Term; Termination. This Agreement will be in effect for the Term and may be renewed or extended by mutual agreement of the parties. Without prejudice to any rights either party may have under this Agreement, in law, equity or otherwise, a party shall have the right to terminate this Agreement if the other party (or in the case of Amplify, an Authorized User) materially breaches any term, provision, warranty or representation under this Agreement and fails to correct the breach within 30 days of its receipt of written notice thereof. Upon termination, Customer will: (a) cease using the Products, (b) return, purge or destroy (as directed by Amplify) all copies of any Products and, if so requested, certify to Amplify in writing that such surrender or destruction has occurred, (c) pay any fees due and owing hereunder, and (d) not be entitled to a refund of any fees previously paid, unless otherwise specified in the Quote. Customer will be responsible for the cost of any continued use of the Products following termination. Upon termination, Amplify will return or destroy any Student Data provided to Amplify hereunder. Notwithstanding the foregoing, nothing shall require Amplify to return or destroy any data that does not include PII, including de-identified information or data that is derived from access to PII but which does not contain PII. Sections 3-13 shall survive the termination of this Agreement.

14. Miscellaneous. This Agreement, including all addenda, attachments, and the Quote, as applicable, constitutes the entire agreement between the parties relating to the subject matter hereof. The provisions of this Agreement shall supersede any conflicting terms and conditions in any Customer purchase order, other correspondence or verbal communication, and shall supersede and cancel all prior agreements, written or oral, between the parties relating to the subject matter hereof. This Agreement may not be modified except in writing signed by both parties. All defined terms in this Agreement shall apply to their singular and plural forms, as applicable. The word "including" means "including without limitation." This Agreement shall be governed by and construed and enforced in accordance with the laws of the state of New York, without giving effect to the choice of law rules thereof. This Agreement will be binding upon and inure to the benefit of the parties and their respective successors and assigns. The parties expressly understand and agree that their relationship is that of independent contractors. Nothing in this Agreement shall constitute one party as an employee, agent, joint venture partner, or servant of another. Each party is solely responsible for all of its employees and agents and its labor costs and expenses arising in connection herewith. Neither this Agreement nor any of the rights, interests or obligations hereunder may be assigned or delegated by Customer or any Authorized User without the prior written consent of Amplify. If one or more of the provisions contained in this Agreement shall for any reason be held to be unenforceable at law, such provisions shall be construed by the appropriate judicial body to limit or reduce such provision or provisions so as to be enforceable to the maximum extent compatible with applicable law. Amplify shall have no liability to Customer or to third parties for any failure or delay in performing any obligation under this Agreement due to circumstances beyond its reasonable control, including acts of God or nature, fire, earthquake, flood, epidemic, strikes, labor stoppages or slowdowns, civil disturbances or terrorism, national or regional emergencies, supply shortages or delays, action by any governmental authority, or interruptions in power, communications, satellites, the Internet, or any other network. Each

party represents and warrants that it has all necessary right, power and authority to enter into this Agreement and to comply with the obligations hereunder.

Customer Privacy Policy

Last Revised: October 30, 2020

Amplify Education, Inc. ("Amplify") is leading the way in next-generation K-12 curriculum and assessment. Amplify's programs provide teachers with powerful tools that help them understand and respond to the needs of every student and use data in a way that is safe, secure, and effective.

This Customer Privacy Policy ("Privacy Policy") or ("Policy") describes how Amplify collects, uses, and discloses personal information and data through the provision of its education products and services ("Products"), including Amplify CKLA, Amplify ELA, Amplify Science, Amplify Math, Amplify Reading, Amplify Fractions, mCLASS and any other product or service that links to this Customer Privacy Policy, to its users (K-12 students, educators, staff and families) and School Customers (School Districts and State Agencies, as defined below). In the course of providing the Products to the Customer, Amplify may collect or have access to "education records," as defined by the federal Family Educational Rights and Privacy Act of 1974 ("FERPA") and personal information that is directly related to an identifiable student (collectively, "Student Data"). This Policy does not apply to Amplify's company website; information collected from users of the webiste is governed by our website privacy policy.

We consider Student Data to be confidential and we collect and use Student Data solely for the purpose of providing our Products to, or on behalf of, our School Customer and for the purposes set out in this Privacy Policy and Customer Agreements. We take numerous measures to maintain the security and confidentiality of Student Data collected or stored by Amplify on behalf of our School Customers, and we enable our School Customers to control the use, access, sharing and retention of the data. Our collection and use of Student Data is governed by our Agreements with our School Customers, including this Privacy Policy, and applicable laws including FERPA, the Children's Online Privacy Protection Act ("COPPA"), as well as other applicable federal, state and local privacy laws and regulations ("Applicable Laws"). With respect to FERPA, Amplify receives Student Data as a "school official" under Section 99.31 of FERPA for the purpose of providing its Products, and such Student Data is owned and controlled by the School Customer.

Amplify is also an early adopter and proud signatory of the Student Privacy Pledge, an industry-wide pledge to safeguard privacy and security of student data. For more information on the pledge, see https://studentprivacypledge.org/.

There may be different contractual terms or privacy policies in place with some of our School Customers. Such other terms or policies may supersede this Policy for information collected or

released under those terms. If you have any questions as to which legal agreement or privacy policy controls the collection and use of your information, please contact us using the information provided below.

1. Definitions. Capitalized terms not defined in this section or above will have the meaning set forth by Applicable Laws.

a. "Agreement" means the underlying contractual Agreement between Amplify and the School Customer.

b. "Authorized Users" means K-12 students, educators, staff and families using Amplify's Products pursuant to an Agreement.

c. "School Customer" means the School District or State Agency that is the party to the Agreement to provide the Amplify Products to the School Customer's Authorized Users.

d. "School District" means a local education agency, school network, independent school, or other regional education system.

e. "State Agency" means the educational agency primarily responsible for the supervision of public elementary and secondary schools in any of the 50 states, the Commonwealth of Puerto Rico, the District of Columbia or other territories and possessions of the United States, as well as a national or regional ministry or department of education in other countries, as applicable.

f. "Student Data" means any information that directly relates to an identifiable current or former student that Amplify collects, receives, or generates in the course of providing the Products to or on behalf of a School Customer. Student Data may include personal information from a student's "educational records," as defined by FERPA.

2. Student Data Collected. Amplify receives Student Data in two ways: (i) from our School Customers to implement the use of our Products and (ii) from Authorized Users.

a. Information provided by our School Customers

- Most of Amplify's educational Products require some basic information about who is in a classroom and who teaches the class. This roster information, including name, email address, grade level, and school ID numbers, is provided to Amplify by our School Customers either directly from the School Customer's student information system or via a third party with whom the School Customer contracts to provide that information.

- Our Customers may also choose to provide additional student demographic data (e.g. socio-economic status, race, national origin) and other school records

(e.g. grades, attendance, assessment results) to Amplify for tailoring

individual learning programs or enabling additional reporting capabilities through Amplify Products. For example, a School District may wish to analyze student literacy assessment results based on English Language Learner status in order to better differentiate classroom instruction, and in that case may provide that data along with other roster information.

b. Information collected through our Products.

- Schoolwork and student generated content. We collect information contained in student assignments and assessments, including information in responses to instructional activities and participation in collaborative or interactive features of our Products. As part of the digital learning experience, some of our Products may enable students to write texts and create and upload images, video and audio recordings.

- Teacher comments and feedback. Some of our Products may enable educators to provide scores, written comments, or other feedback about student responses or student course performance.

c. Other Personal Information Collected

- School Customer Information. We collect personal information when a teacher, administrator or other authorized person associated with a School District or State Agency Customer creates an account or uses our Products or communicates with us. This could include contact information, such as a name, phone number, email address, as well as information about the individual's school and location.

- Parent and Guardian Information. From time to time, we may collect personal information from or about a Student's parent or legal guardian. This information may be provided by a School Customer or directly by the parent or guardian who communicates with us or creates an account.

d. Device and Usage Data.

- Depending on the Product, we may collect certain information about the device used to connect to our Product, such as device type and model, browser configurations and persistent identifiers, such as IP addresses and unique device identifiers. We may collect device diagnostic information, such as battery level, usage logs and error logs as well as usage, viewing and technical information, such as the number of requests a device makes, to ensure proper system capacity for all Authorized Users. We may collect geolocation information from a user's

device, or may approximate device location based on other metrics, like an IP address. Some of our Products use "cookies," Web beacons, HTML5 local storage and other similar technologies to collect and store such data. We use this information to

remember returning users and facilitate ease of login, to customize the function and appearance of the Products, and to improve the learning experience. This information also helps us to track product usage for various purposes including website optimization, to ensure proper system capacity, troubleshoot and fix errors, provide technical assistance and customer support, provide and monitor the effectiveness of our Products, monitor and address security concerns, and to compile analytics for product improvement and other internal purposes.

- With respect to cookies, you may be able to reject cookies through your browser or device controls, but doing so may negatively impact your experience as some features may not work properly. To learn more about browser cookies, including how to manage or delete them, check the "Help," "Tools" or similar section of your browser. If we link or combine device and usage information with personal information we have collected directly from users that relates to or identifies a particular individual, we will treat the combined information as personal information.

- Third party website tracking. Amplify does not track students across third-party websites and does not respond to Do Not Track (DNT) signals. Amplify does not permit third party advertising networks to collect information from or about Students using Amplify educational Products for the purpose of serving targeted advertising across websites and over time and Amplify will never use Student Data for targeted advertising.

3. Use of Student Data. Amplify uses Student Data collected from, or on behalf of, a School Customer to support the learning experience, to provide the Products to the School Customer and to ensure secure and effective operation of our Products, including:

a. to provide and improve our educational Products and to support School Customers' and Authorized Users' activities;

b. for purposes requested or authorized by the School Customer or as otherwise permitted by Applicable Laws;

c. for adaptive or personalized learning purposes, provided that Student Data is not disclosed;

d. for customer support purposes, to respond to the inquiries and fulfill the requests of our School Customers and their Authorized Users;

e. to enforce product access and security controls; and

f. to conduct system audits and improve protections against the misuse of our Products, or to detect and prevent fraud and other harmful activities.

Amplify may use de-identified data as described in Section 5 below.

4. Disclosure of Student Data. We only share or disclose Student Data as needed to provide the Products under the Agreement and as required by law, including but not limited to the following:

a. as directed or permitted by the School Customer;

b. to other Authorized Users of the School Customer entitled to access such data in connection with the Products;

c. to our service providers, subprocessors, or vendors who have a legitimate need to access such data in order to assist us in providing our Products, such as platform, infrastructure, and application software. We contractually bind such parties to protect Student Data in a manner consistent with those practices set forth in this Policy;

d. to comply with the law, respond to requests in legal or government enforcement proceedings (such as complying with a subpoena), protect our rights in a legal dispute, or seek assistance of law enforcement in the event of a threat to our rights, security or property or that of our affiliates, customers, Authorized Users or others;

e. in the event Amplify or all or part of its assets are acquired or transferred to another party, including in connection with any bankruptcy or similar proceedings, provided that successor entity will be required to comply with the privacy protections in this Policy with respect to information collected under this Policy, or we will provide School Customers with notice and an opportunity to opt-out of the transfer of Student Data by deleting such data prior to the transfer; and

f. except as restricted by Applicable Laws or contracts with our School Customers, we may also share Student Data with Amplify's affiliated education companies, provided that such disclosure is solely for the purposes of providing Products and at all times is subject to this Policy.

5. De-Identified Data.

a. Amplify may use de-identified or aggregate data for purposes allowed under FERPA and other Applicable Laws, to research, develop and improve educational sites, services and applications and to demonstrate the effectiveness of the Amplify Products. We may also share de-identified data with research partners to help us analyze the

information for product improvement and development purposes.

b. 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. We de-identify Student Data in compliance with Applicable Laws and in accordance with the

guidelines of NIST SP 800-122. Amplify has implemented internal procedures and controls to protect against the re-identification of de-identified Student Data. Amplify does not disclose de-identified data to its research partners unless that party has agreed in writing not to attempt to re-identify such data.

6. Prohibitions; Advertising; Advertising limitations. Amplify will not:

- sell Student Data to third parties;
- use or disclose Student Data to inform, influence or enable targeted advertising to a student based on Student Data or information or data inferred over time from the student's usage of the Products;
- use Student Data to develop a profile of a student for any purpose other than providing the Products to a School Customer, or as authorized by a parent or legal guardian;
- use Student Data for any commercial purpose other than provide the Products to the School Customer, as authorized by the School Customer or the parent or guardian, or as permitted by Applicable Laws.

Amplify may, from time to time, provide customized content, advertising and commercial messages to School Customers, teachers, school administrators or other non-student users, provided that such advertisements shall not be based on Student Data. Amplify may use Student Data to recommend educational products or services to users, or to notify users about new educational product updates, features, or services.

7. External Third-Party Services.

a. This Privacy Policy applies solely to Amplify's Products and practices. Amplify School Customers and Authorized Users may choose to connect or use our Products in conjunction with third party services and Products. Additionally, our sites and Products may contain links to third party websites or services. This Policy does not address, and Amplify is not responsible for, the privacy, information, or other practices of such third parties. Customers should carefully consider which third party applications to include among the Products and services they provide to students and vet the privacy and data security standards of those providers.

b. Users may be able to login to our Products using third-party sign-in services such

as Clever or Google. These services authenticate your identity and provide you with the option to share certain personal information with us, including your name and email address, to pre-populate our account sign-up form. If you choose to enable a third party to share your third-party account credentials with Amplify, we may obtain personal information via that mechanism. You may configure your accounts on these third party platform services to control what information they share.

8. Security.

a. Amplify maintains a comprehensive information security program and uses industry standard administrative, technical, operational and physical measures to safeguard Student Data in its possession against loss, theft and unauthorized use, disclosure or modification. Amplify performs periodic risk assessments of its information security program and prioritizes the remediation of identified security vulnerabilities. Please see amplify.com/security for a detailed description of Amplify's security program.

b. In the event Amplify discovers or is notified that Student Data within our possession or control was disclosed to, or acquired by, an unauthorized party, we will investigate the incident, take steps to mitigate the potential impact, and notify the School Customer in accordance with Applicable Laws.

c. Amplify's servers are hosted in and managed and controlled by us from the United States and are not intended to subject Amplify to the laws or jurisdiction of any jurisdiction other than that of the United States. If you are a user located outside the United States, you understand and consent to having Student Data collected and maintained by Amplify processed in the United States. United States data protection and other relevant laws may not be the same as those in your jurisdiction. This includes the use of cookies and other tracking technologies as described above.

9. Review and correction.

a. FERPA requires schools to provide parents with access to their children's education records, and parents may request that the school correct records that they believe to be inaccurate or misleading.

b. If you are a parent or guardian and would like to review, correct or update your child's data stored in our Products, contact your School District. Amplify will work with your School District to enable your access to and, if applicable, correction of your child's education records.

c. If you have any questions about whom to contact or other questions about your child's data, you may contact us using the information provided below.

10. Student Data retention. We will retain Student Data for the period necessary to fulfill the

purposes outlined in this Policy and our agreement with that School Customer. We do not knowingly retain Student Data beyond the time period required to support a School Customer's educational purpose, unless authorized by the School Customer. Upon notice from our School Customers, Amplify will return, delete, or destroy Student Data stored by Amplify in accordance with applicable law and customer requirements. We may not be able to fully delete all data in all circumstances, such as information retained in technical support records, customer service records, back-ups and similar business records. Unless

otherwise notified by our School Customer, we will delete or de-identify Student Data after termination of our Agreement with the School Customer.

11. COPPA. We do not knowingly collect personal information from a child under 13 unless and until a School Customer has authorized us to collect such information through the provision of Products on the School Customer's behalf. We comply with all applicable provisions of the Children's Online Privacy Protection Act ("COPPA"). To the extent COPPA applies to the information we collect, we process such information for educational purposes only, at the direction of the partnering School District or State Agency and on the basis of educational institutional consent. Upon request, we provide the School Customer the opportunity to review and delete the personal information collected from students. If you are a parent or guardian and have questions about your child's use of the Products and any personal information collected, please direct these questions to your child's school.

12. Updates to this policy. We may change this Policy in the future. For example, we may update it to comply with new laws or regulations, to conform to industry best practices, or to reflect changes in our product offerings. When these changes do not reflect material changes in our practices with respect to use and/or disclosure of Student Data, such changes to the Policy will become effective when we post the revised Policy on our website. In the event there are material changes in our practices that would result in Student Data being used in a materially different manner than was disclosed when the information was collected, we will notify School Customers affected by the changes via the email contact information provided by the customer and provide an opportunity to opt-out before such changes take effect.

13. Contact us

If you have questions about this Policy, please contact us at:

- Email: privacy@amplify.com
- Mail: Amplify Education, Inc.

  55 Washington St., Ste 800

  Brooklyn, NY, 11201

Attn: General Counsel

Supplemental Disclosures

Nevada. This section applies if you are a resident of the state of Nevada. While Amplify does not sell personal information, as defined in Nevada law, Nevada residents may email a request for no sale of their personally identifiable information to privacy@amplify.com.

California. This section applies to you if you are a resident of the state of California and for purposes of this section the term "personal information" has the meaning provided by the California Consumer Privacy Act (the "CCPA"). Residents of California may be entitled to certain rights with respect to personal information that we collect about them under the CCPA: the Right to Know, the Right to Request Deletion and the Right to Opt-Out of Personal Information Sales. You also have the right to be free of discrimination for exercising these rights. However, please note that if the exercise of these rights limits our ability to process personal information (such as in the case of a deletion request), we may no longer be able to provide you the Products or engage with you in the same manner. To request to exercise your California consumer rights, please contact us at privacy@amplify.com with the subject line "California Rights Request."

Note for students and other users who engage with Amplify in connection with a School Customer's use of Amplify: Because Amplify provides the Products to School Customers as a "School Official," we collect, retain, use and disclose Student Data only for or on behalf of our School Customers for the purpose of providing the Products specified in our agreement with the Customer and for no other commercial purpose. Accordingly, we act as a "service provider" for our School Customers under the CCPA. If you have any questions or would like to exercise your California rights, please contact your School directly.