CUSTOMER PRODUCTS & SERVICES AGREEMENT

This CUSTOMER PRODUCTS & SERVICES AGREEMENT (this "**Agreement**") is made as of May 19, 2022 by and between the Raytown Quality Schools ("**Customer**"), a school district located at 6608 Raytown Rd. Raytown, MO 64133, and AMPLIFY EDUCATION, INC., a Delaware corporation with headquarters at 55 Washington Street, Suite 800, Brooklyn, New York 11201 ("**Amplify**").

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 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. The Data Governance Addendum for District Data of the Raytown C-2 School District, attached hereto as Exhibit A, and Amplify's Customer Privacy Policy attached hereto as Exhibit B, will govern collection, use, and disclosure of Student Data collected or stored on behalf of Customer under this Agreement. To the extent that any provision of the Amplify Customer Privacy Policy conflicts with or contradicts Exhibit A, in letter or spirit, the provisions of Exhibit A shall prevail.

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**. EXCEPT AS EXPRESSED IN EXHIBIT A, DATA GOVERNANCE ADDENDUM FOR DISTRICT DATA OF THE RAYTOWN C-2 SCHOOL DISTRICT, 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. EXCEPT AS EXPRESSED IN EXHIBIT A, DATA GOVERNANCE ADDENDUM FOR DISTRICT DATA OF THE RAYTOWN C-2 SCHOOL DISTRICT AND 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 and EXHIBIT A, Data Governance Addendum for District Data of the Raytown C-2 School District, 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. To the extent that any provision of the Amplify Customer Terms and Conditions (the "T&C") conflict with or contradict with EXHIBIT A, Data Governance Addendum for District Data of the Raytown C-2 School District, in letter or spirit, the provisions of Exhibit A shall prevail. 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.

IN WITNESS WHEREOF, the undersigned are duly authorized to execute this Agreement effective as of the date first set forth above.

_____Raytown Schools_____	AMPLIFY EDUCATION, INC.
By: 	By: Richard Morris
Name: Brian Huff	Name: Richard Morris
Title: Associate Superintendent of C&I	Title: SVP, Finance

EXHIBIT A

Data Governance Addendum for District Data of the Raytown C-2 School District

This Agreement is between **AMPLIFY EDUCATION, INC.** (COMPANY) and **Raytown Quality Schools** (District) and is effective as of the Effective Date.

Definitions.

- **FERPA**: means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1), as amended from time to time.
- **Security Breach (Security Incident)**: means actual evidence of a confirmed unauthorized acquisition of, access to, or unauthorized use of any Student Education Record(s), Personally Identifiable Information, User Data or other district confidential information.
- **Personally Identifiable Information (PII)**: includes but is not limited to (a) student's name; (b) name of the student's parent or other family members; (c) address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; and (e) other indirect personal identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) "medical information" as may be defined in state law; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; (h) nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; (i) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; (j) other financial account numbers, access codes, driver's license numbers; (k) and state- or federal-identification numbers such as passport, visa or state identity card numbers; (l) personal identifiable information as defined by COPPA, including but not limited to online contact information like an email address or other identifier that permits someone to contact a person directly (for example, an IM identifier, VoIP identifier, or video chat identifier), screen name or user name where it functions as online contact information, telephone number, persistent identifier that can be used to recognize a user over time and across different sites (including a cookie number, an IP address, a processor or device serial number, or a unique device identifier), a photo, video, or audio file containing a child's image or voice, geolocation information sufficient to identify a street name and city or town; or other information about the child or parent that is collected from the child and is combined with one of these identifiers.
- **Student Education Record**: means identifiable information, including but not limited to PII, of Subscriber's students that may be considered part of an educational record as defined by FERPA, district policy, and any applicable state law.
- **Anonymized Data**: means any Student Education Record rendered anonymous in such a manner that the student is no longer identifiable. For example, this includes non-identifiable student assessment data and results, and other metadata, testing response times,

scores (e.g. goals, RIT), NCES codes, responses, item parameters, and item sequences that result from the Services.

- **De-identified Data (Pseudonymized Data)**: means a Student Education Record processed in a manner in which the Student Education Record can no longer be attributed to a specific student without the use of additional information, in accordance with applicable laws and the guideline of NIST SP 800-122 . Attributions may include, but are not limited to: name, ID numbers, date of birth, demographic information, location information, and/or any other unique metadata.
- **User Data (District Data)**: any data provided by the District or collected from the District or authorized users, PII, metadata, user content and/or any data part of a student education record that is not anonymized or de-identified. Since the District maintains ownership of all data, this will also be referred to as District Data.

Conditions. Terms used herein shall have the same meaning as in the Amplify Customer Terms and Conditions (the "T&C") unless otherwise specifically provided. To the extent that Company is permitted, under the applicable terms of the Agreement, to subcontract or otherwise delegate its duties and obligations under the Agreement, Company is likewise permitted to subcontract or delegate the performance of corresponding duties and obligations contained in this exhibit, provided however that Company will remain ultimately responsible for such duties and obligations. To the extent that any provision of the T&C conflict with or contradict with this addendum, in letter or spirit, the provisions of this addendum shall prevail.

Designation: Raytown Quality Schools hereby designates Amplify Education, Inc.as a "school official" with "legitimate educational interests" in the District's records, as those terms have been defined under FERPA and its implementing regulations, and Company agrees to abide by the FERPA limitations and requirements imposed upon school officials. Company and District acknowledge that Company will create, access, secure, and maintain Student Education Records to perform the Services as further outlined in the T&C . Company shall not resell Student Education Records or use Student Education Records for targeted student advertising or disclose to third parties any Student Education Records without the written consent of District. District grants permission to Company and its contractors that have executed confidentiality agreements to use Student Education Records for maintaining and providing the Services.

Compliance with Federal and State Confidentiality and Privacy Laws: Company and the District agree and understand that this Agreement must be in compliance with all federal and state confidentiality and privacy laws which includes, but is not limited to: the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99); Protection of Pupil Rights Amendment ("PPRA") (20 U.S.C. § 1232h; 34 CFR Part 98), all of them which may be in effect or amended from time to time, including any successor statute and its implementing regulations and rules. In the event of a conflict between this Agreement and the Confidentiality Laws, the Confidentiality Laws shall control. In the event of a conflict between FERPA and all other Confidentiality Laws, FERPA will control absent clear statutory authority

on controlling law.

- Company shall be responsible for the timing, content, and costs of such legally-required notifications that arise as a result of Company's failure to comply with its obligations as a Service Provider under COPPA, FERPA or other applicable laws. Furthermore, Company shall be responsible for the cost of investigating the above non-compliance, as well as the payment of actual, documented, reasonable costs which may include reasonable legal fees, audit costs, fines, and other fees imposed against the District as a result of the non-compliance. Notwithstanding the foregoing, Company shall be responsible for the costs detailed in this section only to the extent which such failure is attributable to Company, and will not be responsible for costs associated with monitoring that is not legally required.

Data Governance:

Limited Collection, Disclosure, Access and Use:

- Confidentiality: Company and its officers, employees, and agents agrees to hold district data in strict confidence and use the data only for the limited purpose outlined in the T&C .
- Non-Disclosure: Company affirms that its services will be conducted in a manner that does not disclose Customer data to anyone who is not an authorized representative of the Company.
- Data Collection: Company will only collect data necessary to fulfill its duties as outline in this Agreement.
- Data Use: Company will use data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement. The approval to use District data for one purpose does not confer approval to use the data for another or different purpose.
- Access Records: Company will keep true and complete records of any and all District D ata received, exchanged and shared between and amongst its employees, agents, subcontractors and volunteers.
- Sub-processors (Contractors and Agents): Company shall enter into written agreements with all Sub-processors performing functions pursuant to this Agreement, whereby the Sub-processors agree to protect District User Data in a manner consistent with the terms of this Agreement.
- De-Identified Data: De-identified information may be used by the Company for the purposes allowed under FERPA, and for development, research, and improvement of educational sites, services, or applications. Company agrees not to attempt to re-identify de-identified User Data and not to transfer de-identified User Data to any party unless that party agrees in writing not to attempt re-identification.
- Company Access to District Data. The parties agree that Company shall exclusively limit

its employees, contractors, and agents' access to and use of District data to those individuals who have a legitimate need to access District data in order to provide required support of the system or services to the District under the Agreement. Company warrants that all of its employees, contractors, or agents who have such access to confidential District data will be properly vetted, including background checks, to ensure that such individuals have no significant criminal history.

- Employee Obligation: Company shall require all employees and agents who have access to Student Data to comply with terms no less stringent than all applicable provisions of this Agreement. Company agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to District Data.

- Employee Training: Company shall provide periodic security training to those of its employees who operate or have access to the system.

Data Storage/Maintenance. The parties agree that all data collected or held by Company (including but not limited to District students' names and other information) shall be stored within the United States of America. No data may be stored or backed up outside of the continental United States.

Data Security: Company shall maintain and process all data in a secure manner using industry best practices regarding technical, physical, and administrative safeguards. Company utilize appropriate administrative, physical and technical safeguards to secure data from unauthorized access, disclosure, and use. Company will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

Data Encryption. In conducting data transactions and transfers with the District, Company will ensure that all such transactions and transfers are encrypted.

Data Portals. Company warrants and represents that all of its data portals are secured through the use of verified digital certificates.

Data Breach. Company agrees that it will implement industry best practices in administrative, physical and technical safeguards designed to secure User Data and District from unauthorized access, disclosure, or use, which may include, where commercially reasonable or to the extent required by Law, data encryption, firewalls, and physical access controls to buildings and files. In the event Company has a reasonable, good faith belief that an unauthorized party has accessed, or had disclosed to it, User Data that the District provided Company or that Company collected from District or its authorized users, ("Security Incident"), then Company will promptly (as soon as is reasonably possible and in accordance with applicable law), subject to applicable confidentiality obligations and any applicable law enforcement investigation, or if required by Law in such other time required by such Law, notify the District and will use reasonable efforts to cooperate with the District's investigation of the Security Incident.

- If, due to a Security Incident which is caused by the acts or omissions of Company or its agents, employees, or contractors, any third-Party notification of such real or potential data breach is required under law, Company shall be responsible for the

timing, content, and costs of such legally-required notifications. With respect to any Security Incident which is not due to the acts or omissions of Company or its agents, employees, or contractors, Company shall nevertheless reasonably cooperate in the District's investigation and third-party notifications, if any, at the District's direction and expense.

- Company shall be responsible for the cost of investigating any Security Incident determined to be caused by the acts or omissions of Company or its agents, employees, or contractors, as well as the payment of actual, documented costs including reasonable legal fees, audit costs, fines, and other fees imposed against the District as a result of a Security Incident.

- Company shall also be required to outline for the District the steps and processes that Company will take to prevent post-employment data breaches by Company employees after their employment with Company has been terminated.

- Company further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of User Data or any portion thereof, including personally identifiable information and agrees to provide Customer, upon request, with a copy of said written incident response plan.

Cyber Security Insurance. Company will provide to the District a certificate of insurance including Cyber Security Insurance coverage for Data Breach.

Data Dictionary. Company will provide the District with a data inventory that inventories all data fields and delineates which fields are encrypted within Company's platform maintaining collected District data.

Data Ownership. The parties agree that, notwithstanding Company's possession of or physical control over District data, the District maintains ownership and control of all data that the District provides to Company or that Company collects from the District and/or authorized users. Company further agrees that District data cannot be used by Company for marketing, advertising, or data mining, or shared with any third parties unless allowed by law and expressly authorized by the District in writing.

- Parent Access: District has established procedures by which a parent, legal guardian, or eligible student may review education records and correct erroneous information. Company shall cooperate and respond within ten (10) days to the District's request for User Data and/or Education Records held by Company to view or correct as necessary. In the event that a parent or other individual contacts the Company to review any User Data, Company shall refer the parent or individual to the District, who will follow the necessary and proper procedures regarding the requested information.

- Third Party Access: Should a Third Party, including, but not limited to law enforcement, former employees of the District, current employees of the District, and government entities, contact Company with a request for data held by the Company pursuant to the

Services, the Company shall redirect the Third Party to request the data directly from the District and shall cooperate with the District to collect the required information. Company shall notify the District in advance of a compelled disclosure to a Third Party, unless legally prohibited.

Data Handling in the Event of Termination. In the event that the parties terminated their agreement for the provision of Company's services, upon written request any District data within Company's possession or control must be provided to the District or de-identified/deleted, as directed by the District. De-identified data will have all direct and indirect personal identifiers removed, including but not limited to names, addresses, dates of birth, social security numbers, family information, and health information. Furthermore, Company agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party unless that party agrees not to attempt re-identification. If District data is disclosed without de-identifying the same as required herein, written notice shall be provided to the District. If District data is restored from a back-up after the parties' termination of their agreement for Company's services, then that data must also be de-identified/deleted.

Company Visits to District Property. The parties recognize that certain Company employees, contractors, or agents may visit the District's property in order to obtain the necessary information for the provision of Company's services. In the event that a Company employee must be unsupervised on District's property, the parties agree that, before any such visits to the District occur, all visiting Company employees, contractors, or agents must clear both criminal and child abuse & neglect background checks. Company further warrants and agrees that its employees, contractors, or agents who visit the District will not have contact or interact with the District's students. Company will indemnify, defend, and hold the District, its board members, administrators, employees and agents harmless from and against liability for any and all claims, actions, proceedings, demands, costs, (including reasonable attorneys' fees), damages, and liabilities resulting directly, from the acts and/or omissions of Company and/or its employees, contractors, or agents, subcontractors in connection with visits to the District's property as described herein.

Exhibit B

Customer Privacy Policy

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.

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.

HELLOSIGN

Audit Trail

TITLE	(MO) Raytown Quality Schools - DPA
FILE NAME	(MO) Raytown Qual...PY (6-10-22).docx
DOCUMENT ID	3422186957f8e04433169a99f62adfb6ad8ad2c0
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Signed

Document History

SENT	**06 / 13 / 2022** 13:25:42 UTC	Sent for signature to Richard Morris (rmorris@amplify.com) from kjones@amplify.com IP: 69.119.252.145
VIEWED	**06 / 13 / 2022** 14:23:51 UTC	Viewed by Richard Morris (rmorris@amplify.com) IP: 152.39.221.165
SIGNED	**06 / 13 / 2022** 14:24:01 UTC	Signed by Richard Morris (rmorris@amplify.com) IP: 98.116.248.117
COMPLETED	**06 / 13 / 2022** 14:24:01 UTC	The document has been completed.