Amplify

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Amplify Education, Inc. **("Vendor")** are parties to a contract which includes the terms and conditions located at https://amplify.com/customer-terms ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides,K-12 curriculum and assessment products and services("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum dated 10/05/2023. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means student "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act(FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.
2.2. "Vendor" means Amplify Education, Inc..
2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.
2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.
2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.
2.6. "Student" means any person attending or seeking to enroll in an educational agency.
2.7. "Eligible Student" means a student eighteen years or older.
2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.
2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be

handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor EmployeeTraining

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCESshall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES unless done with de-identified data or to improve or develop the Product. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada except as outlined below. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada provided that technical personnel outside of the CONUS or Canada may access software applications containing Protected Information for the purpose of customer support. Such personnel are bound to privacy obligations no less stringent than those of this Addendum.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by

another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe obligations to maintain the privacy and security of Protected Information no less stringent than those required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place and upon request by BOCES thirty (30) days prior to Contract expiration, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall, upon expiration of this Contract, securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de- identified data to any party unless such party has agreed not to re-identify the de-identified data. Vendor may share BOCES de-identified data with research partners for product improvement and development purposes, including research, develop and improve educational sites, services and applications and to demonstrate the effectiveness of Vendor's products.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NISTCybersecurity Framework 1.0;

12.4. equal industry standard practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (AttachmentB);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student Protected Information by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient

way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For Amplify Education, Inc.**
Date 10/4/23	10 / 05 / 2023 Alexandra Walsh **Date**
	Alexandra Walsh, Chief Product Officer

Doc ID: a4c3e29bf37a87fc75cfa6ebfd5730b4739b3980

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insurethatparents haveinformation about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal andteacher data, including Section 2-d of the New YorkStateEducationLaw.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act(FERPA).
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State EducationDepartment, Room 863 EBA,89 Washington Avenue,Albany,New York12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For Amplify Education, Inc.**
Date 10/11/23	**Date** 10 / 05 / 2023
	Alexandra Walsh, Chief Product Officer

Doc ID: a4c3e29bf37a87fc75cfa6ebfd5730b4739b3980

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-

d 8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

Update 6/30/2023: This Privacy Policy has been updated to address new state law data privacy requirements.

We advise you to read this Privacy Policy in its entirety, including the jurisdiction-specific provisions in the appendix. Our Notice At Collection for California residents is available in the Notice for our California Customers.

Customer Privacy Policy: K–12 Schools

Who We Are:

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

Our Products and Services:

Amplify's products support classroom instruction and learning and include Amplify CKLA, Amplify ELA, Amplify Science, Amplify Desmos Math, Desmos Math, Boost Reading, Boost Math, mCLASS, Mathigon, services at teacher.desmos.com (for creating and assigning activities) and student.desmos.com (for use of the activities or curricula as directed by an instructors), and any other product or service that links to this Privacy Policy (together, the "Products").

Our Products are primarily geared towards K–12 students, educators, and staff who use the Products pursuant to an agreement or with the permission of School Districts and State Agencies ("Authorized School Users"). We also provide limited opportunities for teens and parents on behalf of children under 13 ("Child Users") to sign up for an account for at-home use of our Products. See the Appendix for additional information for users of our at-home use of our Products.

What This Privacy Policy Covers:

This Customer Privacy Policy ("Privacy Policy") describes how Amplify collects, uses, and discloses personal information through the provision of Products.

For purposes of this Privacy Policy, "you" and "your" means Authorized Users.

For additional information that applies to the Product(s) that are designed for home use, visit the Appendix–Supplemental Disclosures of this Privacy Policy.

This Privacy Policy does not apply to Amplify's handling of:

- information collected from users of Amplify's company website, which is governed by our Website Privacy Policy.
- applicant data that we process in accordance with our applicant privacy notice.

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 Privacy 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 personal information, please contact us using the information provided below. Unless expressly superseded, this Privacy Policy is incorporated into and is subject to the Agreement that governs your use of the Products.

Our Approach to Student Data Privacy: In the course of providing the Products to our School Customers and their Authorized School Users, Amplify collects, receives, generates, or has access to "Student Data," which is information that directly relates to an identifiable student.

We consider Student Data to be confidential and we collect and use Student Data solely for educational purposes in connection with providing our Products to, or on behalf of, our School Customers, as described in this Privacy Policy and our Agreements. We work to maintain the security and confidentiality of Student Data that we collect or store, and we enable our School Customers to control the use, access, sharing, and retention of Student Data.

Our collection and use of Student Data is governed by our Agreements with our School Customers, including this Privacy Policy, and applicable laws which may include the federal Family Educational Rights and Privacy Act of 1974 ("FERPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), 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.

1. Definitions

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

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

"Authorized Users" means all authorized users of our Products, including Authorized School Users, parents and legal guardians, and children under the age of 13 who are permitted to sign up for our Products only with verifiable consent from their parent or guardian.

"Authorized School Users" means K–12 students, educators, and staff using Amplify's Products pursuant to an Agreement or with the permission of the School District or State Agency.

"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 School Users.

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

"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.

2. What Personal Information Do We Collect?

When you access or use our Products, you may choose to provide us with personal information, including Student Data. This information may be provided to us directly (e.g. when an account is created or through communications with us) or through our Products.

Student Data. Below is a list of the categories of Student Data that may be collected by Amplify or its Products, either directly or through the School Customer's use of the various features and configurations of the Products:

- Identifier and Enrollment Data, such as name, email, school / state ID number, username and password, grade level, homeroom, courses, teacher names.
    - Why? Most of Amplify's Products require some basic information about who is in a classroom and who teaches the class—student or teacher Identifier and Enrollment data. This information 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.
- Demographic Data, such as date of birth, socioeconomic status, race, national origin, and preferred or primary language.
    - Why? To support school instructional and reporting requirements, Amplify's Products allow School Customers to view reports and analyze data using student demographic and other special indicators. For example, a School District may wish to analyze student literacy assessment results based on English Language Learner status to better tailor classroom instruction, and in that case may provide the associated indicator as part of the enrollment information to enable that reporting.
- School Records, such as grades, attendance, assessment results, and Individualized Education Plan status (i.e. whether a plan is in place)
    - Why? Some of our Products support grading assignments and administering formative, diagnostic, and curriculum-based assessments. Teachers use that data to support students' progress in the program or help with instructional decisions. We do not collect specific details from an IEP, nor do we collect health or other sensitive information.
- Schoolwork and Student Generated Content, which includes any information contained in student assignments and assessments, including information in response to instructional activities and participation in collaborative or interactive features of our Products, such as student responses to academic questions and student-written essays, as well as images, video, and audio recordings.
    - Why? 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. For example, in Amplify ELA, students may write essays or submit short-form responses in our platform as part of a lesson on literature. As another example, in Boost Reading, student interactions with reading skills games are recorded to keep track of the student's progress to level up in the program and to provide visibility to teachers on how students are mastering the skills.
- Teacher Comments and Feedback, such as scores, written comments, or other feedback that educators may provide about student responses or student course performance.
    - Why? To enable teachers to track the performance and provide feedback to their students.

Other Data. We may collect the following types of personal information from all other Authorized Users:

- Contact Information, such as name and email address, as well as grade level taught, school name and school location, whether you are a teacher, administrator, or other authorized person that creates an account or uses our Products or communicates with us.

- Account Information, such as customer user login and password, for account creation and access purposes.

- Survey Responses, which you provide in response to surveys or questionnaires.

- 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 (e.g., email open rates), such as the number of requests a device makes, to ensure proper system capacity for all Authorized Users. We may collect IP addresses and use that information to approximate device location to support operation of the Product. To the extent that we collect this information from website visitors who have not signed up for an account, this data is solely used to support operation of the Product and is not linked to Student Data.

    - How? Cookies and Similar Technologies. We collect device and usage data through "cookies," Web beacons, HTML5 local storage, and other similar technologies, which are used in some of our Products.

    - Why? 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 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 compile analytics for product improvement and other internal purposes. Learn how to opt out of cookies and similar technologies by reading the "What Rights and Choices Do You Have?" section of this Privacy Policy below.

3. How Do We Use Personal Information?

Student Data. Amplify uses Student Data for educational purposes, to provide the Products, and to ensure secure and effective operation of our Products, including:

- to provide and improve our educational Products;

- to support School Customers' and Authorized School Users' activities;

- to ensure secure and effective operation of our Products;

- for purposes requested or authorized by the School Customer or Authorized School User or as otherwise permitted by Applicable Laws;

- for adaptive or personalized learning purposes, provided that Student Data is not disclosed to third parties;

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

- to enforce Product access and security controls; and

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

We also use personal information to power the adaptive and personalized learning features of the Products. For example, we may make instructional recommendations to teachers and students based on the student's progress in the program. These recommendations are offered as optional, additional learning support.

Other Data. Amplify may use Authorized User information for the purposes for which Student Data is used as set forth above. Amplify does not use Student Data for marketing purposes, but it may use the personal information of other Authorized Users for marketing in limited circumstances (e.g. to periodically send newsletters and other promotional materials), and as otherwise required or permitted, or as we may notify you at the time of collection. Learn how to opt out of these communications by reading the "What Rights and Choices Do You Have?" section of this Privacy Policy below.

Amplify may use aggregate or de-identified data as described in the Aggregate/De-identified Data section below.

4. To Whom Do We Disclose Personal Information?

Student Data. We disclose Student Data to third parties only as needed to provide the Products under the Agreement, as directed or permitted by the School Customer or Authorized School User, and as required by law. Such disclosures may include but are not limited to the following:

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

- to our service providers, subprocessors, or vendors who have a legitimate need to access such data in order to assist us in providing or supporting 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 Privacy Policy and in accordance with Applicable Laws. List of Amplify subprocessors is available at http://www.amplify.com/subprocessors;

- 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;

- 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 Privacy Policy with respect to information collected under this Privacy Policy, or we will provide the School Customer with notice and an opportunity to opt out of the transfer of such data prior to the transfer; and

- 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.

Other Data. Amplify discloses Authorized User information for the purposes for which Student Data is used as set forth above. Amplify may also disclose Authorized User information as otherwise required or permitted, or as disclosed at the time of collection.

5. Aggregate/De-identified Data

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. Amplify will not attempt to re-identify de-identified data. We may use aggregate information (which is information that has been collected in summary form such that the data cannot be associated with any individual) for analytics and reports. For example, our marketing materials may note the total number of students served by our programs in the prior year, but that information cannot be used to identify any one student. We may also share de-identified or aggregate data with research partners to help us analyze the information for product improvement and development purposes.

Records and information are de-identified when all personal 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. Data 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 Authorized School User, or as authorized by a parent or legal guardian;
- use Student Data for any commercial purpose other than to provide the Products to the School Customer or Authorized School User, or as permitted by Applicable Laws.

Amplify may, from time to time, provide customized content, advertising, and commercial messages to Authorized Users, provided that such advertisements shall not be based on Student Data or directed to K–12 students. Amplify may use de-identified Student Data to recommend educational products or services to School Customers and their Authorized Users (subject to exceptions permitted under applicable law), or to notify such users about new educational product updates, features, or services.

7. External Third-Party Services

This Privacy Policy applies solely to Amplify's Products and practices. Amplify School Customers and other 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 social media plugins (e.g. like or share buttons) as well as links to third-party websites or services. This Privacy 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.

Authorized Users may be able to log in 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

Amplify's servers are hosted, managed, and controlled by us in 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 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 herein. See also Notice for European Economic Area and United Kingdom Customers below.

Student Data

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.

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.

Other Data

Outside of Student Data, Amplify uses commercially reasonable administrative, technical, personnel, and physical measures to safeguard personal information in its possession against loss, theft, and unauthorized use, disclosure or modification.

9. What Rights and Choices Do You Have?

What Choices Do You Have?

Opt-out of Marketing Communications. If you want to stop receiving promotional materials from Amplify, you can email us at privacy@amplify.com or follow the unsubscribe instructions at the bottom of each email.

Opt-out of Cookies and Similar Tracking Technologies. With respect to cookies, you may be able to reject cookies through your browser or device controls. Note that you have to opt-out of cookies on each browser or device that you use. If you replace, change, or upgrade your browser or device, or delete your cookies, you may need to use these opt-out tools again. Please be aware that disabling cookies 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.

What Rights Do You Have With Respect to Student Data?

Review and Correction. 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.

- 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.

- 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.

No 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.

What is our Deletion/Retention Policy?

Upon request, we provide the School Customer the opportunity to review and delete the personal information collected from students.

Student Data Retention. We will retain Student Data for the period necessary to fulfill the purposes outlined in this Privacy Policy and our Agreement with the School Customer. We do not knowingly retain Student Data beyond the time period required to support a School Customer's or Authorized School User's educational purpose, unless authorized by the School Customer or Authorized School User. Upon request, 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 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.

10. COPPA

Except as described in the Appendix, we do not knowingly collect personal information from a Child User unless and until a School Customer or educator has, on behalf of a parent or guardian, authorized us to collect such information to provide the Products. We comply with all applicable provisions of 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. 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.

11. Updates to This Privacy Policy

We may change this Privacy 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 Authorized Users' personal information, including Student Data, such changes to the Privacy Policy will become effective when we post the revised Privacy Policy on our website. In the event there are material changes in our practices that would result in Authorized Users' personal information being used in a materially different manner than was disclosed when the information was collected, with respect to Student Data, we will notify the School Customer, and with respect to other information, we will notify you via email and provide an opportunity to opt out before such changes take effect.

12. Contact Us

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

Email: privacy@amplify.com
Mail: Amplify Education, Inc.
55 Washington St.#800
Brooklyn, NY, 11201
Phone: (800) 823-1969
Attn: General Counsel

To report a security vulnerability, visit https://amplify.com/report-a-vulnerability/.

Appendix – Supplemental Disclosures

1. Notice for Parents/Guardians Regarding Mathigon

While our Products are primarily geared towards School Customers, we do provide an opportunity for children and teens to sign up for a Mathigon account at home—outside of the school context—only with verifiable parental consent from parents or guardians if their child is a Child User.

Please note that most parts of Mathigon can be used without creating an account or providing any personal information that directly identifies you. However, if you are a parent or guardian and would like to authorize your child to sign up for a Mathigon account so that we can offer personalized educational services (e.g. by remembering your child's progress, tailoring our content to your child's interests or abilities, or suggesting what to learn next), please read our Acceptable Use Policy, available at amplify.com/acceptable-use, which explains our verifiable consent process, and then sign up by visiting https://mathigon.org/signup.

What Rights Do You Have? If you are the parent or guardian of a Child User, you may request that we provide for your review, delete from our records, or cease collecting any personal information from your Child User. To exercise these rights, please contact us by sending an email to: help@amplify.com. You may also be able to correct your personal information provided to us, download a copy of all the personal information we have about you, or delete your account via your account settings page. Please note that we may retain certain information as permitted by law. We may also retain cached or archived copies of the information we collect for a certain period of time.

2. Notice for our California Customers

Personal Information We Collect	How We Use Personal Information
Student Data, which includes: • Roster Information • Demographic Data, such as race and national origin • School Records • Account Information • Schoolwork and Student Generated Content • Teacher Comments and Feedback • Device and Usage Data	• To provide and improve our educational Products; • To support School Customers' and Authorized School Users' activities; • To ensure secure and effective operation of our Products; • For purposes requested or authorized by the School Customer or Authorized School Users, or as otherwise permitted by Applicable Laws; • For adaptive or personalized learning purposes, provided that Student Data is not disclosed; • For customer support purposes, to respond to the inquiries and fulfill the requests of our School Customers and their Authorized School Users; • To enforce product access and security controls; and • To conduct system audits and improve protections against the misuse of our Products, or to detect and prevent fraud and other harmful activities.
Authorized Users, which includes: • Contact Information • Account Information • Survey Responses • Device and Usage Data	• For the purposes for which Student Data is used as set forth above; • For marketing purposes in limited circumstances (e.g. to periodically send newsletters and other promotional materials), which will not be based on Student Data or directed to K–12 students

	• As otherwise required or permitted, or as we may notify you at the time of collection.

We do not sell or share your personal information, as described in California law.

We retain your personal information for as long as reasonably necessary for the purposes disclosed in the chart above. Additional information about our retention of Student Data can be found in Section 9 of this Privacy Policy.

Please see the Additional U.S. State Privacy Law Rights section of this appendix for information about your rights pursuant to applicable California law.

Notice of Financial Incentive

As part of our services, there will be opportunities to complete surveys and questionnaires. As an incentive for completing the survey or questionnaire, you can voluntarily provide personal information as an entry into a raffle drawing or to obtain other benefits, discounts, offers, or deals that may constitute a financial incentive under California law ("Financial Incentive"). The categories of personal information required for us to provide the Financial Incentives include: contact information and any other information that you choose to provide when you complete the survey.

Participation is voluntary and you can opt out at any time before the survey is complete. We do not allow students to participate in our surveys.

The value of the personal information we collect in connection with our Financial Incentives is equivalent to the value of the benefit offered.

3. Notice for other U.S. Customers—Additional U.S. State Privacy Law Rights

You have the following rights, where provided under applicable state law, regarding your personal information (each of which is subject to various exceptions and limitations):

- Access. You have the right to request, up to two times every 12 months, that we disclose to you the categories of personal information collected about you; the categories of sources from which the personal information is collected; the categories of personal information sold or shared; the business or commercial purpose for collecting, selling, or sharing the personal information; the categories of third parties with whom personal information was shared; and the specific pieces of personal information collected about you.

- Correction. You have the right to request that we correct inaccurate personal information collected from you, subject to certain exceptions allowed under applicable law.

- Deletion. You have the right to request that we delete the personal information that we maintain about you, subject to certain exceptions. Even after the deletion of your account, some personal information may remain on our servers, such as in technical support logs, server caches, data backups, or email conversations. These will be automatically deleted after a reasonable amount of time, unless we are legally required to retain information for longer, or unless there is a legitimate business reason (e.g. security and fraud prevention or financial record-keeping). We are not required to delete any information which has been aggregated or de-identified in accordance with Section 5.

- No Discrimination. You have the right not to be discriminated against for exercising these rights.

- Appeals. You have a right to appeal decisions concerning your ability to exercise your consumer rights.

- Submission of Requests. You may exercise the above rights by emailing us at privacy@amplify.com. Note that we may deny certain requests, or fulfill a request only in part, based on our legal rights and obligations. For example, we may retain personal information as permitted by law, such as for tax or other record keeping purposes, to maintain an active account, and to process transactions and facilitate customer requests.

- Authorized Agent. You may designate an authorized agent to make a request on your behalf. When submitting the request, please ensure the authorized agent identifies himself/herself/itself as an authorized agent and can show written permission from you to represent you. We may contact you directly to confirm that you have authorized the agent to act on your behalf and confirm your identity.

- Verification. Whether you submit a request directly on your own behalf, or through an authorized agent, we will take reasonable steps to verify your identity prior to responding to your requests. The verification steps will vary depending on the sensitivity of the personal information and whether you have an account with us.

  Note for students and other Authorized Users who engage with Amplify in connection with a School Customer's use of Amplify: Because Amplify provides the Products to School Customers and Authorized Users as a "School Official," we collect, retain, use, and disclose Student Data only for or on behalf of our School Customers and Authorized Users for educational purposes, including the purpose of providing the Products specified in our Agreement with the School 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.

4. Notice for European Economic Area and United Kingdom Customers

If you represent a school in the United Kingdom or European Economic Area, you can review our standard template DPA with attached SCCs here. If the school would like to enter into that DPA (and attached SCCs) with Amplify, please send an email to privacy@amplify.com with the following information about the school: (i) name, (ii) address, (iii) telephone number, (iv) signatory name, (v) signatory title, and (vi) signatory email address, and (vii) teacher.desmos.com account usernames. We will then send the school's signatory a copy of the DPA for electronic signatures and arrange for signature by Amplify's authorized representative.

Amplify collects personal data for the purposes described in Section 3 of this Privacy Policy. We rely on the following lawful bases for our processing activities:

- Consent;
- Pursuant to a contract with the user of our Products;
- To comply with our legal obligations; or
- When we have a legitimate interest in doing so, which is not outweighed by the risks to the individual.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Amplify.

New York Data Privacy and Security Addendum

The purpose of this Addendum is to facilitate educational agency compliance with New York State Education Law section 2-d and regulations promulgated thereunder ("NY Education Privacy Laws"), including the requirement under section 121.2 of the regulations that each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with federal and state law and the educational agency's data security and privacy policy.

This Addendum supplements Amplify's Terms and Conditions for use of Amplify products licensed by the educational agency available at https://amplify.com/customer-terms (the "Agreement").

For the purposes of this Agreement, "breach," "commercial or marketing purpose," "disclose or disclosure," "education records," "encryption," "personally identifiable information," "release," "student data," "teacher or principal data," "unauthorized disclosure or unauthorized release" will be as defined by NY Education Privacy Laws.

1. Bill of Rights for Data Privacy and Security. In accordance with section 121.3 of the regulations, Amplify hereby agrees to comply with the parents bill of rights for data privacy and security ("bill of rights") as promulgated by the educational agency. In accordance with section 121.3(c) of the regulations, see Attachment A for supplemental information to the bill of rights.

2. Data Security and Privacy Plan. In accordance with Section 121.6 of the regulations, see Attachment B for Amplify's data security and privacy plan.

3. Third Party Contractor Compliance. In accordance with Section 121.9 of the regulations, Amplify as a third-party contractor that will receive student data or teacher or principal data, represents and covenants that Amplify will:
    - (1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;
    - (2) comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part 121;
    - (3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
    - (4) not use the personally identifiable information for any purpose not explicitly authorized in its contract;
    - (5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the

educational agency; or (ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the

information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

- o (6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
- o (7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and
- o (8) not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
- o Where Amplify engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on Amplify by state and federal law and this Agreement shall apply to the subcontractor.

4. Reports and Notifications of Breach and Unauthorized Release. In accordance with section 121.10 of the regulations, Amplify will:
   - o promptly notify the educational agency of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach;
   - o cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.
   - o where a breach or unauthorized release is attributed to Amplify, Amplify shall pay for or promptly reimburse the educational agency for the full cost of such notification. In compliance with this section, notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.

5. General.
   - o The laws of the State of New York shall govern the rights and duties of Amplify and the educational agency.
   - o If any provision of the contract or the application of the contract is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of the contract which can be given effect without the invalid provision or application.
   - o This Agreement controls over any inconsistent terms or conditions contained within any other agreement entered into by the parties concerning student,

teacher and principal data.

ATTACHMENT A EDUTECH

SUPPLEMENTAL INFORMATION FOR THE BILL OF RIGHTS

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract:

   The purposes for which Amplify will use student, teacher, or principal data are described in Amplify's Customer Privacy Policy, available at h ttps://amplify.com/customer-privacy/.

2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d):

   Amplify requires all subcontractors or other authorized persons with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.

3. The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed):

   The Agreement will last for the time period described in the applicable purchasing document, unless earlier terminated in accordance with the Agreement. Student, teacher, or principal data will be returned or destroyed in accordance with whichever is the sooner of 1) the period necessary to fulfill the purposes outlined in Amplify's Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, or 3) the educational agency's option and direction.

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected:

   A parent, student, eligible student, teacher or principal may contact the education agency directly to discuss the correction of any such erroneous information. If Amplify receives a request to review student data in Amplify's possession directly from such a party, Amplify agrees to refer that individual to the educational agency and to notify the educational agency within a reasonable time of receiving such a request. Amplify agrees to work cooperatively with the education agency to permit a parent, student, eligible student, teacher or principal to review student, teacher, or principal data that has been shared with Amplify and correct any erroneous information therein.

5. Where the student data or teacher or principal data will be stored, described in such a

manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated:

Amplify leverages Amazon Web Services (AWS) as its cloud hosting provider. Further information regarding Amplify's security program can be found on Amplify's Information Security page at
https://amplify.com/security.

6. Address how the data will be protected using encryption while in motion and at rest:

   In transit: Amplify encrypts all student personal information in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes.

   At rest: Amplify encrypts student personal information at rest using the industry-standard AES-256 encryption algorithm.

ATTACHMENT B EDUTECH

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

DATA SECURITY AND PRIVACY PLAN

In accordance with Section 121.6 of the regulations, the following is Amplify's data security and privacy plan:

1. Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy:

   Amplify's privacy policy, available at amplify.com/customer-privacy/, outlines how Amplify's practices enable its customers to control use, access, sharing and retention of personal information in compliance with FERPA and other applicable privacy laws and regulations. Upon request, Amplify will also certify compliance with the educational agency's data security and privacy policy.

2. Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract:

   Administrative, operational and technical safeguards and practices to protect PII under the Agreement are described in Amplify's Information Security page at https://amplify.com/security.

3. Demonstrate that it complies with the requirements of Section 121.3(c) of this Part 121:

   The supplemental information required by Section 121.3(c) of this Part 121 are attached to this Addendum as Attachment A.

4. Specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access:

   Amplify has a comprehensive information security training program that all employees and individuals with access to Amplify systems undergo upon initial hire or engagement, with an annual refresher training. We also provide information security training for specific departments based on role.

5. Specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected:

   Amplify may use independent contractors engaged by Amplify in the ordinary course of business or for purposes that are incidental or ancillary to the provision of services under the Agreement. Amplify requires all subcontractors with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.

6. Specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency:

   If there has been an unauthorized release, disclosure or acquisition of the educational agency's student, teacher, or principal data, Amplify will notify the educational agency in accordance with applicable laws and regulations. Such notification will include the following steps: Amplify will notify the educational agency after Amplify determines that the educational agency's student, teacher, or principal data were released, disclosed, or acquired without authorization, (a "Security Incident"), without unreasonable delay, 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, release, 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.

7. Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

   Upon the termination or expiration of the Agreement and upon the educational agency's request, student, teacher, or principal data will be returned, transitioned, and/or destroyed in accordance with 1) Amplify's Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, and 3) in accordance with the educational agency's direction.

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by Amplify Education, Inc.(the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") which include the terms and conditions located here https://amplify.com/customer-terms and the Addendum dated 10/05/2023 (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in a format mutually agreed to by the parties and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored in the United States]; provided that technical personnel may access software applications containing BOCES' data for the purpose of providing customer support. The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law

Section 2-d and other applicable law.

Signature: Alexandra Walsh

Date: 10 / 05 / 2023