JEFFERSON • LEWIS • HAMILTON • HERKIMER • ONEIDA

BOARD OF COOPERATIVE EDUCATIONAL SERVICES

Contract Addendum
Protection of Student, Teacher, and Principal Data

1. Applicability of this Addendum

The Jefferson, Lewis, Hamilton, Herkimer, Oneida BOCES ("BOCES"), an educational agency, and Amplify Education, Inc.("Vendor") are parties to a contract, Amplify Price Quote Number: Q-206545-1 attached hereto as Attachment D, dated 3/20/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, educational products and services, as described in Attachment D ("Product"). BOCES' use of the Product results in Vendor receiving student, teacher, or principal personally identifiable information as defined in federal and state statute, including New York Education Law Section 2-d and this Addendum. 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 "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.

2.2 "This Contract" means the underlying contract as modified by this Addendum.

2.3 "Protected Information", as applied to student data, means "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. "Protected Information", as applied to Teacher or Principal Data means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2.4 "Breach" means the unauthorized acquisition, access, use, or disclosure of Protected Information by or to a person not authorized to acquire, access, use, or receive the Protected Information.

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 Policies on Data Security and Privacy and the Parent's Bill of Rights for Data Privacy and Security, copies of which are Attachment B to this Addendum.

5. Vendor Employee Training

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 to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

Notwithstanding the foregoing, Vendor may, from time to time, provide customized content, advertising and commercial messages to BOCES, teachers, school administrators or other non-student users, provided that such advertisements shall not be based on Student Data. Vendor 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. De-Identified Data

Protected Information is 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. Vendor will de-identify Student Data in compliance with applicable laws and in accordance with the guidelines of NIST SP 800-122.

Vendor 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 Vendor's products. Vendor may also share de-identified data with research partners to help us analyze the information for product improvement and development purposes. Vendor will not disclose de-identified data to its research partners unless that party has agreed in writing not to attempt to re-identify such data.

8. Ownership and Location of Protected Information

8.1 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.

8.2 BOCES shall have access to the BOCES' 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.

8.3 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 or as outlined in this Addendum. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

8.4 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. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

9. 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 BOCES.

10. 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 the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract

and all applicable New York State and federal laws.

11. Protected Information and Contract Termination

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

11.2 Upon expiration of this Contract without a successor agreement in place, upon request of BOCES, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

11.3 Vendor shall thereafter 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.

11.4 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.

11.5 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 also agrees not to attempt to re-identify such data.

11.6 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.

12. Data Subject Request to Amend Protected Information

12.1 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).

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

13. Vendor Data Security and Privacy Plan

13.1 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.

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

a. align with the NIST Cybersecurity Framework 1.0;

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

c. 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 (Attachment B);

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

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

f. 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;

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

h. 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

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

14. Additional Vendor Responsibilities

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 may subject the vendor to a monetary civil penalty and shall be a breach of this Contract:

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

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

14.3 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 less than three (3) business day prior to disclosure, unless such notice is expressly prohibited by the statute or court order;

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

14.5 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);

14.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of Protected Information that is student data 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

14.7 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.

Dated: 5/31/2023

Michele A. Traynor

For the Jefferson-Lewis BOCES

Richard Morris

For the Vendor

JEFFERSON • LEWIS • HAMILTON • HERKIMER • ONEIDA

BOARD OF COOPERATIVE EDUCATIONAL SERVICES

Attachment A - Supplemental Information about this Contract

CONTRACTOR	**Amplify Education, Inc.**
PRODUCT	**See Attachment D**
PURPOSE DETAILS	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 BOCES. The product or services are used to provide See Attachment D .
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.
DATA DESTRUCTION INFORMATION	The agreement expires See Attachment D . Upon expiration of this Contract without a successor agreement in place, upon request of BOCES, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES. Vendor shall thereafter 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. 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.

DATA ACCURACY INFORMATION	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

Dated: 5/31/2023

Richard Morris

Michele A. Gaynor

For the Jefferson-Lewis BOCES

For the Vendor

Attachment B - Parents' Bill of Rights for Data Privacy and Security and BOCES Data Security Policy

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student, as well as eligible students, defined as those students who are eighteen years or older, are entitled to certain rights with regard to their child's personally identifiable information (PII), as defined by Education Law §2-d. Jefferson-Lewis BOCES Policy 6001 contains a plain-English summary of such rights. Vendor specifically acknowledges receipt of Parents' Bill of Rights for Data Privacy and Security and BOCES Data Security Policy, which are attached hereto, and understands its legal obligations as provided therein.

[ATTACH POLICIES]

Dated: 5/31/2023

Michele A. Gaynor

For the Jefferson-Lewis BOCES

Richard Morris

For the Vendor

Attachment C – Vendor's Data Security and Privacy Plan

The BOCES Parents Bill of Rights for Data Privacy Security, receipt of which is acknowledged as Attachment B to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

[INSERT LINKS OR TEXT, AS PROVIDED BY THE VENDOR]

Dated: 5/31/2023

Michele A. Traynor
For the Jefferson-Lewis BOCES

Richard Morris
For the Vendor

Policy

PERSONNEL 4243

DATA SECURITY AND PRIVACY

I. Purpose

This policy addresses Jefferson Lewis Hamilton Herkimer Oneida BOCES' ("BOCES") responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources.

II. Policy Statement

It is the responsibility of the BOCES:

1. To comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;
2. To maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the BOCES' mission;
3. To protect personally identifiable information (PII), and sensitive and confidential information from unauthorized use or disclosure;
4. To address the adherence of its vendors with federal, state and BOCES' requirements in its vendor agreements;
5. To train its users to share a measure of responsibility for protecting BOCES' data and data systems;
6. To identify its required data security and privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and
7. To communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

III. Standard

BOCES will utilize the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

IV. Scope

1. The policy applies to BOCES employees, and also to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to BOCES' data and/or data systems.
2. This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of the educational agency and it addresses all information, regardless of the form or format, which is created or used in support of the activities of BOCES.
3. This policy shall be published on the BOCES' website along with the Parents Bill of Rights for Data Security and notice of its existence shall be provided to all employees and Users.

V. Compliance

The Chief Executive Officer and/or District Superintendent is responsible for the compliance of BOCES' programs and offices with this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and program offices will be directed to adopt corrective practices, as applicable.

VI. Oversight

The BOCES' Data Protection Officer shall annually report to the Board on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to Education Law §2-d.

VII. Data Privacy

1. Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.
2. Data protected by law must only be used in accordance with law and regulation and BOCES policies to ensure it is protected from unauthorized use and/or disclosure.
3. BOCES will take steps to minimize collection, processing and transmission of PII.
4. BOCES has established a Data Governance Team to manage its use of data protected by law. The Data Protection Officer and the Data Governance Team will, together with program offices, determine whether a proposed use of PII would benefit students and educational agencies, and ensure that PII is not included in public reports or other public documents, or otherwise publicly disclosed.

5. No student data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulation.
6. BOCES will not sell PII 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.
7. The identity of all individuals requesting PII, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with BOCES' procedures.
8. It is BOCES' policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, BOCES shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.
9. Contracts with third parties that will receive or have access to PII must include a Data Privacy and Security Plan that outlines how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.
10. All third party contracts that will receive or have access to PII are required to comply with the BOCES Parent's Bill of Rights for Data Privacy and Security.

VIII. Incident Response and Notification

1. BOCES will respond to data privacy and security critical incidents in accordance with its Technology and Safety, Information Security Breach, Education Records, Student Technology and Safety policies and regulations.
2. All breaches of data and/or data systems will be reported by the Data Governance Team to the Data Protection Officer.
3. All breaches of PII or sensitive/confidential data must be reported to the Data Protection Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any BOCES sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.
4. State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of PII. Upon receiving a report of a breach or

unauthorized disclosure, the Data Governance Team and other related professionals will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

IX. Technology and Safety and Student Technology and Safety Policies

1. Users must comply with the Technology and Safety and Student Technology and Safety polices and regulations in using BOCES resources.
2. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with BOCES User Access Policy.
3. Accounts will be removed, and access will be denied for all those who have left the BOCES or moved to another department.
4. Users must comply with the password requirements as outlined in the Acceptable Use Policy.
5. All remote connections must be made through managed points-of-entry in accordance with the User Access Policy

X. Training

All users of BOCES data, data systems and data assets must annually complete the information security and privacy training offered by the BOCES. Information security and privacy training will be made available to all users. Employees must complete the training annually.

Jefferson-Lewis-Hamilton-Herkimer-Oneida Board of Cooperative Educational Services
Legal Ref: Education Law §2-d; NYCRR T. 8, Ch. II, Subch. E, Pt. 121; Family Educational Rights and Privacy Act; Individuals with Disabilities Education Act
Cross Ref: Policy 4240, 4242, 5050, 5250, 6001

Adopted: May 13, 2020

Policy

STUDENTS 6001

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information (PII), as defined by Education Law §2-d. This document contains a plain-English summary of such rights.

1. A student's PII 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 educational records maintained by the Jefferson Lewis BOCES. This right of inspection is consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA) and policy. In addition to the right of inspection of the student's educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record. The rights of parents and students under FERPA can be accessed at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn. In addition to review, these rights include how to challenge the accuracy of the content of a student's educational record.
3. State and Federal Laws protect the confidentiality of PII, 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 New York State is available for review at the following website:

   http://www.nysed.gov/common/nysed/files/programs/data-privacy-security/ inventory-of-data-elements-collected-by-nysed_0.pdf.

   The list may also be made available by writing to:

   Office of Information & Reporting Services
   New York State Education Department Room 863 EBA
   89 Washington Avenue
   Albany, New York 12234
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

   Data Protection Officer
   20104 State Route 3
   Watertown, New York 13601
   (315) 779-7000

OR

Chief Privacy Officer
New York State Education Department 89 Washington Avenue
Albany, New York 12234
Email: Privacy@NYSED.gov

6. Supplemental information will be maintained by BOCES for each contract the BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data. Those contracts with a third-party a will include information addressing the following:

   a. The exclusive purposes for which the student data or teacher or principal data will be used.

   b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations.

   c. The duration of the contract, including the contract's expiration date and description of what happens to the student data or teacher and principal data upon expiration of the agreement.

   d. If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

   e. Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

   a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;

   b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

   c. Not use educational records for any other purpose than those explicitly authorized in the contract;

   d. Not disclose PII to any other party except as outlined in the contract (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later

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

e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;

f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

g. Notify the Jefferson-Lewis BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;

i. Provide a signed copy of this Bill of Rights to the Jefferson-Lewis BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

9. BOCES shall publish on its website the Parents Bill of Rights for Data Privacy and Security and any Supplement to the Bill of Rights for any contract or other written agreement with a third-party contractor that will receive PII.

Jefferson-Lewis-Hamilton-Herkimer-Oneida Board of Cooperative Educational Services
Legal Ref: Education Law §2-d; 8 NYCRR Part 121; Children's Internet Protect Act

(CIPA). Adopted: September 17, 2014; Modified: May 13, 2020; Modified: October 20,

2021

Amplify.

Information Security at Amplify

Information Security at Amplify

Last Revised: June 18, 2020

1. Service Overview

As a provider of technology solutions to schools, Amplify's commitment to data privacy and security is essential to our organization. This overview of Amplify's Information Security Program describes physical, technical and administrative safeguards Amplify implements to protect student personal information in our care. While it is not possible to completely secure against all threats, we believe that by following the industry best practices described below, we provide appropriate protections for student personal information in our care.

Company Profile

Amplify Education, Inc. (Amplify) is a privately held company founded in 2000 as Wireless Generation. Amplify's products include curriculum and instruction, assessment and intervention, professional development services and consulting services for K-12 education.

Service Hosting

Amplify leverages Amazon Web Services (AWS) as its cloud hosting provider. Within AWS, Amplify utilizes Virtual Private Clouds (VPCs), which provide an isolated cloud environment within the AWS infrastructure. External network traffic to a VPC is managed via gateway and firewall rules, which are maintained in source code control to ensure that the configuration remains in compliance with Amplify security policy. In addition, the production VPCs and the development VPCs are isolated from each other and maintained in separate AWS accounts.

2. Policies & Standards

Information Security Program

Amplify maintains a comprehensive information security program based on the industry recognized ISO27002 series and the NIST 800-53 Rev. 4 family of information security controls. These provide a robust framework of best practices from which an organization can build its security policies and protocols based on identified risks, compliance requirements, and business needs. They cover critical practice areas, including access control, configuration management, incident response, security training, and other information security domains.

Governance

Amplify's Information Security Committee has primary responsibility for the development, maintenance, and implementation of the Amplify information security program. The Information Security Committee is responsible for all information risk management activities within the company and is composed of technology, business and legal leaders from the organization. The Committee includes a dedicated Director of Security and a program manager to oversee, direct and coordinate its activities.

Policy Execution

Adherence to the internal Amplify information security policy is an obligation of every Amplify employee. Amplify conducts a series of internal monitoring procedures to verify compliance with internal information security policies, and all Amplify employees undergo annual criminal background checks. In addition, any third-party contractors who come into contact with systems that may contain student personal information are contractually bound to maintain security and privacy of the data.

3. Data Access Controls

Access Control

Amplify's access control principles dictate that all student personal information we store on behalf of customers is only accessible to district-authorized users and to a limited set of internal Amplify users who may only access the data for purposes authorized by the district. Districts maintain control over their internal users and may grant or revoke access.
In limited circumstances and strictly for the purposes of supporting school districts and maintaining the functionality of systems, certain Amplify users may access Amplify systems with student personal information. All such access to student personal information by Amplify technicians or customer support requires both authentication and authorization to view the information.

Encryption

- *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.

4. Application Security by Design

Building the right roles into applications

Permissions within Amplify applications are designed on the principle that school districts control access to all student data. To facilitate this, Amplify applications are designed so that roles and permissions flow from the district to the individual user. For example, applications that offer schools a way to collect and report on assessment results have a web interface that requires district administrators to authorize individuals to view student personal information.

Security controls within applications are used to ensure that the desired privacy protections are technically enforced within the system. For example, if a principal is supposed to see only the data related to his or her school, Amplify ensures that, throughout the design and development process, our products restrict principals from seeing records for any students outside his or her school.

To make sure Amplify applications properly enforce permissions and roles, our development teams conduct reviews early in the design process to ensure roles and permissions are an essential component of the design of new applications.

Building security controls into applications

Amplify applications are also developed to minimize security vulnerabilities and ensure industry-standard application security controls are in place.

As part of the development process, Amplify has a set of application security standards that all applications handling student personal information are required to follow, including:

- Student personal information is secured using industry standard encryption when in transit between end-users and Amplify systems.
- Applications are built with password brute-force attack prevention.
- User sessions expire after a fixed period of time

We also conduct manual and automated static code analysis as well as dynamic application security testing to preemptively identify vulnerabilities published by industry leaders such as

OWASP (Open Web Application Security Project).

5. Proactive Security

Vulnerability Assessments

Amplify periodically engages a security consulting firm to conduct risk assessments, aimed at identifying and prioritizing security vulnerabilities. The Information Security Committee coordinates remediation of the vulnerabilities. The security consulting firm also provides ongoing advice on current risks and advises on remediation of vulnerabilities and incident response.

Penetration Testing

Amplify engages third-party firms to continually conduct application penetration testing. The purpose of this testing is to test for application security vulnerabilities in the production environment. We work with third party penetration testing program partners. Third-party testing involves a combination of automated and manual testing.

Vulnerability Management

Amplify maintains a comprehensive vulnerability management program based on the proactive functions of the NIST Cybersecurity Framework Core:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

The implementation of these functions includes:

- Risk Assessment conducted by industry-leading third parties
- External vulnerability scans conducted by industry-leading third parties
- Internal vulnerability scans and configuration scans
- Intrusion Detection Systems

- Penetration testing conducted by third parties

Endpoint Security

Access to production systems at Amplify is restricted to a limited set of internal Amplify users to support technical infrastructure, troubleshoot customer issues, or other purposes authorized by the district. In addition, Amplify is completing implementation of two-factor authentication methods for access to all production systems. Two-factor authentication involves a combination of something only the user knows and something only the user can access. For example, two-factor authentication for administrative access could involve entering a password as well as entering a one-time passcode sent via text message to the administrator's mobile phone. The use of two-factor authentication reduces the possibility that an unauthorized individual could use a compromised password to access a system.

Infrastructure Security

Network filtering technologies are used to ensure that production environments with student personal information are properly segmented from the rest of the network. Production environments only have limited external access to enable customers to use our web interfaces and other services. In addition, Amplify uses firewalls to ensure that development servers have no access to production environments.

Other measures that Amplify takes to secure its operational environment include system monitoring to detect anomalous activity that could indicate potential attacks and breaches.

Security Training

At Amplify, we believe that protecting student personal information is the responsibility of all employees. We implemented a comprehensive information security training program that all employees undergo upon initial hire, with an annual refresher training. We also provide information security training for specific departments based on role.

6. Reactive Security

Monitoring

Amplify implemented intrusion detection and prevention systems (IDS/IPS) to monitor the network and report anomalous activity for appropriate resolution.

Incident Response

Amplify maintains a comprehensive Security Incident Response Policy Plan, which sets out roles, responsibilities and procedures for reporting, investigation, containment, remediation and notification of security incidents.

7. Compliance

Audits

In addition to penetration testing and other proactive security testing and monitoring outlined above, Amplify has successfully completed a SOC 2 Type 2 examination of controls relevant to security. The examination is formally known as a Type 2 Independent Service Auditor's Report on Controls Relevant to Security. It was conducted by Schellman & Company, LLC and covers the period from April 1, 2019 to March 31, 2020. The report states that Amplify's systems meet the criteria for the security principle and opine on management's description of the organization's system and the suitability of the design of controls to protect against unauthorized access, use, or modification.

The Type 2 report also opines on the operating effectiveness of controls over the review period. This means that our auditors confirmed that we have continued to follow established security controls over the period of time of the review.

Certifications

SOC 2: Amplify successfully completed the SOC 2 Type 2 examination of controls relevant to security (see above, under "Audits").

Privacy

Amplify's products are built to facilitate district compliance with applicable data privacy laws, including FERPA and state laws related to the collection, access and review and disclosure of student data. Amplify's Customer Privacy Policy describes the types of information collected and maintained on behalf of our school district customers and limitations on use and sharing of that data. 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.

8. Supporting Documentation

In the course of customer security assessment, the following documentation can be provided by Amplify upon customers' request:

- Penetration Testing Report
- SOC 2 Type 2 Report

Amplify's Subprocessors

For more information about Amplify's data collection, handling, use and disclosure practices, please see our Customer Privacy Policy.

Student Data

Amplify's subprocessors of Student Data are:

Subprocessor	Purpose
Amazon Web Services, Inc.	Cloud hosting services
Blackboard, Inc.	Video conferencing and attendance tracking for tutoring services
dbt Labs, Inc.	Run database queries
Desmos Studio, PBC.	Customer support services for Desmos Classroom
Egnyte,	Secure file exchange

Inc.	
Global Grid for Learning, PBC.	Secure rostering
Google LLC	Cloud hosting services
Google LLC (Looker)	Data warehouse analytics
MongoDB, Inc.	Database hosting for Mathigon.org and Desmos Classroom
Qualfon Data Services Group, LLC	Customer support services
Snowflake, Inc.	Database hosting
Twilio, Inc (Sendgrid)	Email delivery for Mathigon.org
Zendesk, Inc.	Support messaging for Desmos Classroom

This list may be periodically updated to the extent we contract with additional subprocessors, in all cases in accordance with our Customer Privacy Policy and with appropriate written agreements.

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.

- (6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
- (7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and
- (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;
- 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:
   - 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;
   - cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.
   - 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.**
   - The laws of the State of New York shall govern the rights and duties of Amplify and the educational agency.
   - 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.
   - 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.

ACKNOWLEDGED AND ACCEPTED:

BY: _____

Name: Catherine MacKay
Title: President and Chief Operating Officer

ATTACHMENT A

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 https://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

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.

2023 - 2024

Amplify.

Price Quote

Amplify

55 Washington Street, Suite 800
Brooklyn, NY 11201
Phone: (800) 823-1969
Fax: (646) 403-4700

Quote #: Q-206545-1
Date: 3/20/2023
Expires On: 4/19/2023

Customer Contact Information
Lynn Gaffney
Jefferson Lewis BOCES
Lowville Central School Dist
315-779-7043
lgaffney@boces.com

Amplify Contact Information
Alisa Weis
Inside Sales Representative
(480) 510-6703
aweis@amplify.com

PRODUCT	QUANTITY	PRICE	TOTAL DISCOUNT	TOTAL PRICE
Boost Reading Site License (501-750 students) - 1yr (2023-2024)	1.00	$10,750.00	$0.00	$10,750.00
TOTAL			$0.00	$10,750.00

SHIPPING AND HANDLING	SHIPPING COST	TOTAL DISCOUNT	TOTAL PRICE
Amplify Shipping and Handling	$0.00	$0.00	$0.00

TOTAL DISCOUNT $0.00
GRAND TOTAL $10,750.00

Michele Tiapus
Approving Signature

Scope and Duration

Payment Terms:

- This Price Quote (including all pricing and other terms) is valid through Quote Expiration Date stated above.
- Payment terms: net 30 days.
- Prices do not include sales tax, if applicable.
- Pricing terms in the Price Quote are based on the scope of purchase and other terms herein.
- The Federal Tax ID # for Amplify Education, Inc. is 13-4125483. A copy of Amplify's W-9 can be found at: http://www.amplify.com/w-9.pdf

License and Services Term:

- Licenses: 07/01/2023 until 06/30/2024.
- Services: 18 months from order date. Unless otherwise stated above, all training and other services purchased must be scheduled and delivered within such term or will be forfeited.

Special Terms:

- FOR SHIPPED MATERIALS:
  - Expedited shipping is available at extra charge.
  - Print materials and kits are non-returnable and non-refundable, except in the case of defective or missing materials reported by Customer within 60 days of receipt.
- FOR SERVICES:
  - Training and professional development sessions cancelled with less than one week notice will be deemed delivered.

How to Order Our Products

Amplify would like to process your order as quickly as possible. Please visit amplify.com/ordering-support to find all the information you need for submitting your order. We accept the following forms of payment: purchase orders, checks, and credit card payments (Visa, MasterCard, Discover and American Express). In order for us to assist you, please help us by following these instructions:

Please include these three documents with your order:

- Authorized purchase order or check
- A copy of your Price Quote
- A copy of your Tax-Exemption Certificate

If submitting a purchase order:

To expedite your order, please visit amplify.com/ordering-support where you can submit your signed purchase order. You can also email a purchase order to IncomingPO@amplify.com or fax it to (646) 403-4700. Purchase Orders can also be mailed to our Order Management Department at the address below.

If submitting your order via credit card:

- Please email Accountsreceivable@amplify.com to request a secure credit card payment link

If submitting your order via sending a check:

- Please mail your documents directly to our Order Management Department and notify your sales representative of the check number and check amount.
- Please note that mailing a check can add up to two weeks of processing time for your order. For faster processing of your order, please submit your order via Purchase Order or Credit Card Authorization Form.

The information requested above is essential to ensure the smooth completion of your order with Amplify. Failure to submit documents will prevent your order from processing.

Our Order Management Department is located at 55 Washington Street, Suite 800, Brooklyn, NY 11201. Please note that mailing any documents can result in delays of up to two weeks. **For faster processing of your order, we recommend you submit a purchase order via our website: amplify.com/ordering-support.**

This Price Quote is subject to the Customer Terms & Conditions of Amplify Education, Inc. attached and available at amplify.com/customer-terms. Issuance of a purchase order or payment pursuant to this Price Quote, or usage of the products specified herein, shall be deemed acceptance of such Terms & Conditions.

Terms & Conditions

1. Scope. Amplify Education, Inc. ("Amplify") and Customer wish to enter into the 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 (this "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 to access and use the Products solely in the U.S. during

the Term for the number of Authorized Users specified in the Quote for whom Customer has paid the applicable fees to Amplify. "Authorized User" means an individual teacher or other personnel employed by Customer, or an individual student registered for instruction at Customer's school, whom Customer permits to access and use the Products subject to the terms and conditions of this Agreement, and solely while such individual is so employed or so registered. Each Authorized User's access and use of the Products shall be subject to Amplify's Terms of Use available through the Products, in addition to the terms and conditions of this Agreement, and violations of such terms may result in suspension or termination of the applicable account.

3. Restrictions. Customer shall access and use the Products solely for 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, or sell, 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 therein 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 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 http://www.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 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, including software, source code, assessment instruments, research, designs, methods, processes, customer lists, training materials, product documentation, know-how and trade secrets, in whatever form ("Confidential Information"). 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 Customer is subject to federal and local laws relating to the protection of personally identifiable information of students ("PII"), including the Family Educational Rights and Privacy Act ("FERPA"), and that Amplify is obtaining such PII as a "school official" under Section 99.31 of FERPA for the purpose of providing the Products hereunder. Subject to the terms and conditions of this Agreement, Amplify will not take any action to cause Customer to be out of compliance with FERPA or applicable state laws relating to PII. Amplify's Customer Privacy Policy at http://www.amplify.com/customer-privacy will govern collection, use, and disclosure of information collected or stored on behalf of Customer under this Agreement.

10. Customer Materials. 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 http://www.amplify.com/customer-requirements.

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

12. Limitation of Liability. IN NO EVENT SHALL AMPLIFY BE LIABLE TO CUSTOMER OR TO ANY AUTHORIZED USER FOR ANY INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE OR COVER DAMAGES, DAMAGES FOR LOST PROFITS, LOST DATA OR LOST BUSINESS, OR ANY OTHER INDIRECT DAMAGES, EVEN IF AMPLIFY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, AMPLIFY'S ENTIRE LIABILITY TO CUSTOMER OR ANY AUTHORIZED USER ARISING OUT OF PERFORMANCE OR NONPERFORMANCE BY AMPLIFY OR IN ANY WAY RELATED TO THE SUBJECT MATTER OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE AGGREGATE OF CUSTOMER'S OR ANY AUTHORIZED USER'S DIRECT DAMAGES UP TO THE FEES PAID BY CUSTOMER TO AMPLIFY FOR THE AFFECTED PORTION OF THE PRODUCTS IN THE PRIOR 12 MONTH-PERIOD. UNDER NO CIRCUMSTANCES SHALL AMPLIFY BE LIABLE FOR ANY CONSEQUENCES OF ANY UNAUTHORIZED USE OF THE PRODUCTS THAT VIOLATES THIS AGREEMENT OR ANY APPLICABLE LAW OR REGULATION.

13. Term; Termination. This Agreement will be in effect for the duration specified in the Quote 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 the cost of any continued use of Products following such termination. Upon termination, Amplify will return or destroy any PII of students provided to Amplify hereunder. Notwithstanding the foregoing, nothing shall require Amplify to return or destroy any data that does not include PII, including de-identified information or data that is derived from access to PII but which does not contain PII. Sections 3-13 shall survive the termination of this Agreement.

14. Miscellaneous. This Agreement, including all addendums, attachments and the Quote, as applicable, constitutes the entire agreement between the parties relating to the subject matter hereof. The provisions of this Agreement shall supersede any conflicting terms and conditions in any Customer purchase order, other correspondence or verbal communication, and shall supersede and

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

We are delighted to work with you and we thank you for your order!