



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 this contract and the DISTRICT Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, 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 DISTRICT 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; shall not be used by Vendor or its Assignees to develop or improve a product or service except to the extent such use is permitted by applicable law; 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 DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.

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

foregoing, as a vendor to multiple state and district customers, Vendor cannot allow direct access to its systems. Upon request, Vendor will provide results of the most recent third party security assessment report that is relevant to District's data.

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

7.4 All Protected Information shall remain in the continental United States (CONUS) or Canada; provided that technical personnel may access software applications containing Protected Information for the purpose of customer support. Any Protected Information must be stored solely in data centers in CONUS or Canada except as otherwise provided herein.

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 DISTRICT.

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 and if such entity has access to Protected Information, 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 materially similar 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.

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 DISTRICT request, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT.

10.3 Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors as well as any and all Protected Information maintained on

behalf of Vendor in secure data center facilities in accordance with the Contract.

10.4

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 third party agrees not to attempt to re-identify the data.

10.6 Upon request, Vendor and/or its subcontractors or assignees will provide a certification to DISTRICT 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 DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2 Vendor will cooperate with DISTRICT 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.

a.

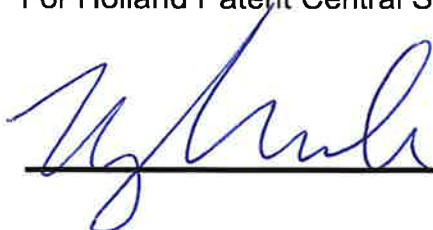
13. Additional Vendor Responsibilities

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 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 DISTRICT 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 DISTRICT 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 as follows: In transit: Vendor 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.
- 13.6 At rest: Vendor encrypts student personal information at rest using the industry-standard AES-256 encryption algorithm.
- 13.7 Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data that is 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
- 13.8 Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full out-of-pocket cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

For Holland Patent Central School District



Nancy Nowicki
Assistant Superintendent

For Amplify Education, Inc.

Richard Morris

Richard Morris
SVP, Finance

Date:

Date: 09/07/2023

Attachment A – Parents’ Bill of Rights for Data Security and Privacy

Holland Patent Central School District Parents’ Bill of Rights for Data Privacy and Security

1. A student’s personally identifiable information (PII) cannot be sold or released by the District/BOCES for any commercial or marketing purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by the District/BOCES. This right of inspection is consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). In addition to the right of inspection of the 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. NYSED will develop policies and procedures pertaining to this right some time in the future.
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 the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to file complaints with the District/BOCES about possible privacy breaches of student data by the District’s/BOCES’ third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints regarding student data breaches should be directed to Dr. Cheryl Venettozzi, Superintendent, Holland Patent Central School District, 9601 Main Street, Holland Patent, NY 13354. Phone: 315-865-7200. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. The complaint process is under development and will be established through regulations to be proposed by NYSED’s Chief Privacy Officer, who has not yet been appointed.

Policy

SUPPORT OPERATIONS

5071

PURPOSE, USE AND ADMINISTRATION OF DISTRICT DIGITAL INFORMATION SYSTEMS

I. Scope of Policy

- A. Digital information systems are important to achieving the District's educational goals and conducting business operations in an efficient manner. The Board's goal is to provide students and staff with digital technology tools that are appropriate to support the District's instructional goals and operational needs, consistent with a wise use of the District's financial resources.
- B. When used in this Policy, the term "digital information systems" includes computers of any size and form factor (including smartphones and tablets), network servers, routers, cables, interactive white boards, video conferencing equipment, switches, and software that is owned, leased, or licensed by the District, or that the District has the use of through a cooperative educational services agreement (CoSer), and that is used to create, modify, store, or transmit information in a digitized form.
- C. This Policy applies to the use of all District-managed devices, including mobile devices such as laptop computers and digital tablets, whether the equipment is used by staff, students, or members of the public. References to District-managed devices shall include devices owned by the District and devices that may continue to be owned by the BOCES but are assigned to the District for use within the District under District supervision.
- D. This Policy also applies to the use of digital devices that are not District-managed devices but are used to access and connect to the District's network, whether the device is owned or used by a staff member, student, or member of the public.
- E. Anyone who uses any part of the District's digital information systems is expected to comply with the standards of use set forth in this Policy, whether that person is a staff member (employees and volunteers), student, contractor, or member of the public (including parents and community members).
- F. In addition to the standards set forth in this Policy for use of the District's digital information systems, users of those systems must comply with all other board-adopted policies and related regulations, including but not limited to, the Code of Conduct, the Internet Safety Policy, and the Equal Opportunity and Nondiscrimination Policy.

II. District Accountability for Use of Digital Information Systems

- A. The Board recognizes the District's responsibility to monitor the use of its digital information assets to insure that those assets are used for their intended purposes, and

Attachment C – Vendor’s Data Security and Privacy Plan

The DISTRICT Parents Bill of Rights for Data Privacy Security, a signed copy of which is included as Attachment A to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

https://amplify.com/site-privacy/?_gl=1%2Ae4xztf%2A_qa%2ANjk1ODY3NjAyLjE2OTA5OTM4Njc.%2A_qa_KB37BKPPF6%2AMTY5MTU5MDkxNy4yLjEuMTY5MTU5MTA2MC41OS4wLjA.

Email: privacy@amplify.com

Mail: Amplify, 55 Washington St., Ste 800, Brooklyn, NY, 11201 Attn:
General Counsel

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:
 - o (1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;
 - o (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;
 - o (3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
 - o (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.

SUPPLEMENTAL INFORMATION FOR THE BILL OF RIGHTS

- A parent, student, eligible student, teacher or principal may contact the educational 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 educational 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 contractors 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.