

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

- (a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

- (d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of the MLSA. Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption., and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.
- (b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

Vendor's administrative, operational and technical safeguards and practices to protect PII under the MLSA are described in Amplify's Information Security Policy, attached hereto.

- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (e) Vendor _____ will ☒ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:
 - (i) the parent or eligible student has provided prior written consent; or

- (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice 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 personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.
- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

- (1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- (2) Parents have the right to inspect and review the complete contents of their child's education record.
- (3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- (4) A complete list of all student data elements collected by the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the 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 in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

BY THE VENDOR:

Steven Zavari

Signature

Steven Zavari

Printed Name

Senior Vice President and General Manager, STEM

Title

9/3/2020

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT BETWEEN ERIE 1 BOCES AND AMPLIFY EDUCATION, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Amplify Education, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Amplify Science

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Vendor 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 Vendor and the educational agency, Vendor takes full responsibility for the actions of any such parties.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on the effective date of the MLSA and expires on the date the MLSA expires without renewal, or is terminated in accordance with the terms of the MLSA.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.



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