

Title: Executive Director

Title: CEO & President

Address: 355 Harlem Rd

Address: 22700 Alcalde Rd Cupertino, CA
95014

West Seneca, NY 14224

Date: 5/31/2023

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.. Erie 1 BOCES will provide Vendor with a copy of its policy. 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.

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:

MaiaLearning meets all state information data security requirements and has implemented all of the security standards outlined in CIPA. MaiaLearning is GDPR compliant and complies fully with the requirements of the Federal Family Educational Rights and Privacy Act of 1974. MaiaLearning is in compliance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. Sec. 6501-6506 ("COPPA") and consistent with the Privacy Policy of the Website, students under thirteen should not create accounts on MaiaLearning™. The only exception is when MaiaLearning™ has data sharing agreements in place and in which districts consent to usage on behalf of the student.

We have implemented several layers of security and encryption. Data in our system is encrypted at rest and on the fly. Student information is protected with encryption, and all traffic runs over https. Server access is protected with VPN tunnels and Two Factor Authentication. Access to pupil data requires authentication using personal ID's and passwords. User passwords are encrypted within Maia Learning and cannot be printed or seen by users at any level.

Our security protocol governs data breaches. This includes:

- *Verify the authenticity of the issue*
- *Take actions to ensure continued access is blocked*
- *Simultaneously notify impacted parties*
- *Assess root cause and ensure no further vulnerabilities exist*
- *Assess full scope and notify impacted parties*

(MaiaLearning Data Privacy and Security Plan included as an attachment)

- (b) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (c) 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.
- (d) Vendor [*check one*] _____ will ___x___ 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.

- (e) 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.
- (f) 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)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

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: MaiaLearning, Inc.

DocuSigned by:
Satish Mirle
F7777B884BC8447...
Signature

Satish Mirle
Printed Name

CEO and President
Title

5/31/2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

 ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
 BETWEEN
 ERIE 1 BOCES AND [*MAIALEARNING, INC.*]

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with [*MaiaLearning, Inc.*] which governs the availability to Participating Educational Agencies of the following Product(s):

[[MaiaLearning HS Platform, MaiaLearning MS Platform, MaiaLearning District Platform, MaiaDocs, Maia SMS Text Module, System Setup/SIS Plugin, Maia Essay Dev Tools, Maia Skills and Strengths Assessments, SAT & ACT Test Prep, MaiaLearning Social Emotional Learning (SEL) Curriculum, and MaiaLearning College and Career Readiness (CCR) Curriculum.

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 will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA.*

Direct access to the application administrative functions is prohibited from the external world and only allowed through 2-factor authentication for a restricted set of personnel from our development and network operations center teams on a need basis. The restricted set of personnel will be trained by our CTO on the new NYS 2-d data security and data privacy laws and will abide by the provisions of the law.]

]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on **July 1, 2023 and expires on June 30, 2026.**
- 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, or any de-identified 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.

Attachment A: MaiaLearning Data Privacy and Security Measures:

Compliance with Privacy Laws

MaiaLearning, Inc. complies fully with the requirements of the federal Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S.C. Sec. 1232g (FERPA), the Student Online Personal Information Protection Act, Assembly Bill No. 1584 codified in Education Code Section 49073.1, and all other federal and state guidelines applicable and adopted in accordance therewith. Personally identifiable information received by MaiaLearning, Inc. will be used solely for legitimate educational interests.

Pursuant to FERPA, MaiaLearning, Inc. may disclose your personal information in cases where we believe that such disclosure is reasonably necessary to meet the requirements of an applicable and enforceable law, regulation, or government request, to comply with a judicial order or lawfully issued subpoena, in connection with a health or safety emergency, to address fraud, security, or technical issues, or to enforce the applicable Terms of Use.

Pursuant to AB 1584, Pupil records entered into accounts on the Website by students of the Local Educational Agency (LEA) shall continue to be the property of, and under the control of, the LEA. Students may retain possession and control of or transfer such accounts to personal accounts upon by following instructions from within their account. In the event of an unauthorized disclosure of records, we will promptly notify the affected parent, legal guardian, or eligible pupil and LEA and take appropriate mitigation efforts. Pupil records shall not be retained upon completion of the terms of the contract.

In compliance with federal guidelines, personal information acquired by the MaiaLearning, Inc. will not be used to engage in targeted advertising on any site, service, or application when the targeting of the advertising is based upon any of the acquired personal information. Pursuant to FERPA all users may, through the proper processes described herein, seek to amend education records believed to be inaccurate. However, in cases where data was provided by your school or school district, you may not be able to update, delete, or otherwise modify the data, except through the applicable procedures of the school or school district.

Further, in compliance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. Sec. 6501-6506 ("COPPA") and consistent with the Privacy Policy of the Website, students under thirteen should not create accounts on MaiaLearning™. The only exception is when MaiaLearning™ has data sharing agreements in place and in which districts consent to usage on behalf of the student.

MaiaLearning Security Standards:

- *Service Data is encrypted in transit to and from MaiaLearning facilities when traveling over public networks (HTTPS, SFTP)*
- *The PII (as defined under the laws of the United States) portions of the Service Data is encrypted at rest*
- *MaiaLearning employs administrative, physical and technical safeguards to secure they system, including, but not limited to, restricting production systems to "need to access" personnel.*
- *The infrastructure provider used to provide the Services is currently Amazon Web Services, Inc. ("AWS"). AWS states that it is ISO*

27001, ISO 27017, ISO 27018, PCI DSS Level 1, FIPS 140-2, SOC 1, SOC 2 and SOC 3

- *External HTTP encryption is managed using AWS load balancers*
- *Database storage is encrypted at rest*
- *Development and production systems are maintained on separate networks with separate VPN access, and such networks are kept separate.*
- *Command line access to machines is provided via VPN, and commands are logged*
- *MaiaLearning takes part in annual independent third-party security scan and audit*
- *MaiaLearning maintains an Incident Response Plan that includes prompt and appropriate notification to impacted parties*

Security Measures

MaiaLearning, Inc. takes appropriate precautions to protect your information. Your account information is located on a secured server behind a firewall. We encrypt information being sent to or from our servers using secure socket layer technology (SSL). (To learn more about SSL, go to http://en.wikipedia.org/wiki/Secure_Sockets_Layer).

-