

## 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:

## MAIALEARNING INC

# Hosting Details for MaiaLearning Confidential

January 2020

---

## MAIALEARNING INC

### EXECUTIVE SUMMARY

#### Objective

This document addresses key aspects of hosting of MaiaLearning.

#### Scalability

The MaiaLearning Platform is developed on a LAMP Stack with a content management system in the underlying structure. The entire system is hosted in the cloud using Amazon Web Services.

The architecture of the hardware stack includes multiple availability zones, with each zone supporting a minimum of 4 high end Servers. Both availability zones are run in an active / active configuration, with incoming traffic distributed across the availability zones in a round robin manner. Each zone is set to auto-scale such that when the zone capacity of servers exceeds a certain cpu and memory utilization, new servers are added on an on demand basis. New servers are spun up within minutes and added to the availability zone and start to serve traffic.

Our database makes use of Amazon Aurora. This is a MySQL-compatible relational database engine that combines the speed and availability of high-end commercial databases with the on-demand scalability of a cloud infrastructure. Amazon Aurora provides 5X the throughput of standard MySQL running on the same hardware. This consistent performance is at least equivalent to commercial databases and in most cases far exceeded them. The instance size that we have picked for MaiaLearning can support close to 125,000 reads and 25,000 writes per second. The database deployment topology also includes Read replicas of the database that are setup for all reporting purposes and reduce any load on active traffic from end users. Aurora also comes with autoscaling for storage, and automatically adds in increments of 10GB and can scale up to 64TB.

For non-database data management, we use Amazon S3 buckets with 100's of terabytes of extensibility. As the application for MaiaLearning runs, static content will be cached using Amazon ElastiCache that will increase performance and scalability.

FTP servers are setup for school districts to deposit data files. The FTP servers are set to autoscale so that as traffic increases, we have more servers spin up automatically. Access to the servers is managed

through Amazon Identify and Access Management (IAM) roles and Amazon Directory Services (similar to Microsoft Active Directory). Once a file is loaded to the FTP server, they are moved to an S3 bucket. When the file is uploaded into S3 an event triggers the processing functions that are written as AWS Lambda functions. The functions upload student information into the database. The advantage of using AWS Lambda functions is that they run on-demand and

---

---

## MAIALEARNING INC

don't run when not needed. They are perfect for these types of processes where you might need 300 parallel running import jobs from 9am-10am and then only 4 parallel jobs the rest of the day.

### Security

Security is paramount in the setup of any online system. In the case of MaiaLearning this is something that we have paid extra attention to. There are several layers of security in definition of the system architecture.

### System Security

System security is a key requirement from protecting information. The production servers are hosted in a private subnet in a virtual private cloud that is inaccessible directly from the internet. Special VPN access is required to access the servers in the VPC. The VPN accounts are accessible with username and password combination with 2 factor authentication (2FA) generated by Google Authenticator on the users mobile device. For schools to deposit files into our FTP servers, we enable Identity and Access Management that use data encryption keys. User accounts are managed through AWS Directory Services thereby protecting the FTP server from direct access.

The FTP servers are set up as write-only, or blind-write. This means that while a school can write files to the system they can't see files they, or anyone else, have uploaded.

Amazon Aurora is integrated with AWS Identity and Access Management (IAM) and provides the ability to control the actions that AWS IAM users and groups can take on specific Amazon Aurora resources (e.g., DB Instances, DB Snapshots, DB Parameter Groups, DB Event Subscriptions, DB Options Groups). In addition, we can tag Amazon Aurora resources, and control the actions that IAM users and groups can take on groups of resources that have the same tag (and tag value). Amazon will keep Amazon Aurora databases up-to-date with the latest patches automatically.

### Data Security

Student data **MUST** be protected. All data we store in our database is encrypted at rest. The encryption is done on the fly at the database tier. Amazon Aurora is configured to encrypt the databases using keys we create and control through the AWS Key Management Service (KMS). On a database instance running with Amazon Aurora encryption, data stored at rest in the underlying storage is encrypted, as are the automated backups, snapshots, and replicas of the cluster. The application connects to Amazon Aurora using SSL (AES-256) connections to secure the data in transit.

The entire site is run on HTTPS with TLS with the highest strength ciphers enabled. Certificates use 2048 bits for encryption. Any request coming in on HTTP are redirected in the browser to HTTPS. There will be multiple integrations to 3rd party services. These include CSU Application, Community College Integration, Common Application, eTranscripts with Parchment and Assessment products. All of these integrations are made available over secure communication protocols with HTTPS. All API integrations to MaiaLearning will also occur using HTTPS protocol and with an extra layer of authentication of API Keys and Secrets. Our policy is to only accept valid keys for HTTPS communication with no exceptions.

---

## MAIALEARNING INC

### Application Security

MaiaLearning is front-ended with Akamai's acceleration platform. This provides us with consistent response times through out the world. As part of application security, MaiaLearning includes:

- Origin Obfuscation and protection through Akamai's SiteShield. This prevents any malicious attacker from directly going after the Origin Servers
  - Akamai's KONA site Defender. This blocks top 10 OWASP vulnerabilities and includes protection for volumetric attacks and SLOW Post attacks.
  - DNS protection through Akamai's FastDNS for volumetric DNS attacks while giving DNS resolution close to the client
  - Enterprise Threat Protector that protects from any malware that can be installed on our servers from going out to control and command centers through DNS queries and exfiltrating data.
  - Amazon's application firewall as a second layer firewall closer to the origin.
  - Access to Application is prohibited from the external world and only allowed through 2 factor authentication for
- restricted set of personnel from our development and network operations center teams.

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 on the new NYS 2-d data privacy laws. MaiaLearning is front-ended with Akamai's acceleration platform. This provides us with consistent response times through out the world.

### Security Audit

At MaiaLearning, we engage with an independent 3rd party security company to perform audits on both the infrastructure and application. The audits run for over 2 months where they run penetration tests across all of our APIs. Once complete, remediations are recommended, that we incorporate into the platform. Our next audit is scheduled for summer.

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 and will continue to provide

training on the federal and state laws governing confidentiality of such data prior to their receiving access.

### Security Protocols

The privacy of our customers' data is our utmost concern and we take our obligations to safeguard it very seriously. We take our obligation to keep you informed if any data is compromised equally seriously.

Our security protocol for any potential security incident involving user data requires us to:

1. Verify the authenticity of the issue.

---

---

### MAIALEARNING INC

2. Once verified, we take all actions to ensure that continued unauthorized access is blocked.
3. Simultaneously, we notify potential impacted parties.
4. Next, we assess root cause and ensure no other portions of the system are vulnerable to the same attack.
5. Finally, we assess the full scope of the issue and notify impacted parties: this notice.

---

---

### MAIALEARNING INC

#### Disaster Recovery

MaiaLearning is setup across multiple availability zones with real time replication of the database to an Aurora standby instance. Given that we have Multi-AZ DB instances running, snapshots are taken from the standby.

The most critical part of the system is the database. Amazon RDS continuously monitors the health of Amazon Aurora database and the underlying EC2 instance. On database failure, Amazon RDS will automatically restart the database and associated processes. Amazon Aurora does not require crash recovery replay of database redo logs, greatly reducing restart times. Amazon Aurora also isolates the database buffer cache from the database process, allowing the cache to survive a database restart.

On instance failure, Amazon Aurora uses RDS Multi-AZ technology to automate failover to one of up to 15 Amazon Aurora Replicas in any of three Availability Zones. If no Amazon Aurora Replicas have been provisioned, in the case of a failure, Amazon RDS will attempt to create a new Amazon Aurora DB instance automatically.

Each 10GB chunk of the database volume is replicated six ways, across three Availability Zones. Amazon Aurora storage is fault-tolerant, transparently handling the loss of up to two copies of data without

affecting database write availability and up to three copies without affecting read availability. Amazon Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and replaced automatically.

Amazon RDS creates a storage volume snapshot of the DB instance. This process backs up the entire DB instance, not just individual databases. Amazon RDS provides two methods for creating these backups: automated backups and manual (customer-initiated) DB snapshots. Amazon RDS backup storage for each region is composed of the automated backups and manual DB snapshots for that region and is equivalent to the sum of the database storage for all instances in that region.

In addition to the daily automated backup, Amazon RDS archives database change logs. This enables us to recover our database to any point in time during the backup retention period, up to the last five minutes of database usage.

The web servers running MaiaLearning run on high end reserved instances. We have a Multi-AZ deployment with active/active instances. If a server goes offline due to hardware failures, the autoscale feature will ensure automatic start of new instances immediately. MaiaLearning will be initially rollout with 50% additional capacity. When large districts are to be on-boarded, we will proactively increase the capacity of the infrastructure in anticipation of this web traffic.

Each Amazon Availability Zone is a physically separate datacenter from the other Availability Zones in that Region. The Availability Zones are linked using using dark fiber for maximum performance. In the event of a catastrophic

---

## MAIALEARNING INC

failure of all Availability Zones in a Region, we can use the database backups and Cloud Formation templates to restore the entire site within 6 hours in another Amazon Region which will be in another part of the country.

### Quality Assurance and Release Processes

MaiaLearning is a highly available system and the processes governing this are strict. As product features are enhanced and bugs are fixed, it is imperative that such releases be managed in way as to not impact the function of the platform.

- All products features have requirement specifications and scoped. Such specifications are tracked to completion in JIRA, our agile tracking system. Feature releases are pre-planned.
- Features are developed by the development team and rolled into a development staging area
- A thorough testing of the features is completed by a QA team, and regression testing is performed on the platform so that no other part of the site is impacted.
- QA approved code is moved to a preproduction environment. The QA team will re-run regression tests in the preproduction environment. . The feature is then handed of to customers for validation of the new features and sign off.
- Exceptions for releasing any code mid-week are made to only handle critical bugs. Lower priority bugs will be bundled in to a feature release, or a maintenance release schedules ahead of time.

The same process outlined for quality assurance of the system is followed for maintenance releases.

- Approved code is slated for a release. All releases will happen during Friday evenings so as to not impact any user. The actual code roll out process is done one availability zone at a time so that there is no downtime associated to a release. Database snapshots are taken just before code is pushed to production.
- In the event of a release issue, code is rolled back along with the database snapshot to pre-release state. **Monitoring**

A key aspect to high availability is ensuring that we know proactively what is happening on the site. As part of the system setup of MaiaLearning, we are instituting real time monitoring. This includes:

- Resource monitoring including CPU, Memory and Disk utilization • Application log monitoring for errors
- Database monitoring for any integrity of data
- Apache log monitoring for user logins and malicious activities

---

## MAIALEARNING INC

- Storage monitoring for utilization
- Active user and performance monitoring
- Active dashboards will be setup for operations teams for monitoring • Monitoring of application firewall for OWASP vulnerabilities

### MaiaLearning Inc. Policies and Procedures for 1584 Compliance

#### 1. Pupil records continue to be the property of and under the control of the school district.

Student records are the property of the schools. For each school, there is a school administrator account with access to all school records. The system also provides a district administrator role, that enables visibility into all student accounts in the district. Schools and MaiaLearning staff have visibility into all accounts on a need basis for the purposes of ensuring proper functioning and monitoring utilization. Schools and MaiaLearning staff follow strict privacy and security protocols when accessing such data. MaiaLearning Inc. does not provide user information to 3rd parties for any non-contracted purpose. We specifically never provide user information to any 3rd party for marketing or advertising purposes.

#### 2. A description of the means by which pupils may retain possession and control of their own pupil-generated content, if applicable, including options by which a pupil may transfer pupil generated content to a personal account

Students see their accounts and can edit or delete information they enter, so they control it. They can download their resumes and essays (with reviewers' comments). Content they enter (except calendar



entries, and Journals or Galleries marked “private”) is visible to their families, counselors, current teachers, and administrators with the appropriate roles. Students should maintain their own copies of files they upload to Portfolios. Download of academic and career plans as pdf’s will be added to MaiaLearning.

**3. A prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract.**

Other than pupils themselves, the only people who have access to pupil records are school counselors, teachers, and administrators, and the pupil’s parents or legal guardians.

In our privacy statement, we specify that “we may disclose student information in cases where we believe such disclosure is reasonably necessary to 1) meet the requirements of an applicable and enforceable law, regulation, or governmental request, 2) address fraud, security, or technical issues, or 3) to enforce applicable Terms of Use.” Thus far we have not had to disclose any student information for any of these purposes.

**4. A description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil’s records and correct erroneous information.**

Students, parents, and legal guardians may view pupil information in the Student Information app, and report

---

---

**MAIALEARNING INC**

erroneous data to their schools and districts. Such data will be corrected within the SIS systems at the districts and on the next data update feed in MaiaLearning. The PII data updates are limited to what districts send to MaiaLearning. All other user generated data can be updated by the user.

**A description of the actions the third party will take—including the designation and training of responsible individuals—to ensure the security and confidentiality of pupil records**

---

---

MaiaLearning provides limited student information to contracted third party partners such as Human eSources or Parchment, as required for proper operation of our platform. This does not allow the third party to access a student’s account. MaiaLearning provides any necessary content (such as a student’s identification, graduation year, and college application list, for Parchment) through calls to the third party software’s API.

These partners receive partial information, insufficient to identify a student:

- Human eSources - Learning Styles assessment
- O\*NET (Dept. of Labor) - Holland Interest Profile assessment • Super College - Scholarships
- Parchment can identify the student.

Parchment Protocol: The personal or institution identifying information is stored in secured facilities with restricted access, and protected by protocols and procedures designed to ensure the security of such information. In addition, all individuals who have access to such information are trained in the maintenance and security of such information, and Parchment limits access of such information by its employees to the minimum information reasonably required in order to provide prompt, high quality services.

**5. A description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records;**

In the unlikely event of unauthorized disclosure of pupil records, we will notify the school administrators immediately via email and phone calls. We will also email pupils and their legal guardians (where we have the necessary contact information) when we become aware of such an event. We will take immediate steps to mitigate any harm or damages resulting from such disclosure.

**6. A certification that a pupil's records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced (NOTE: This requirement does not apply to pupil-generated content if the pupil chooses to establish or maintain an account with the third party for the purpose of storing that content, either by retaining possession and control of their own pupil-generated content, or by transferring pupil-generated content to a personal account.**

When a student graduates from his/her school, the account remains active for four years. However, if the school or district requests deletion of data under the control of the school or district, the information will be deleted based on the specific request of school or district.

**7. A description of how the district and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act (FERPA)**

Students and their parents can view student account content on MaiaLearning (including courses, grades, test scores, etc). They must contact the school directly if they believe this school-provided information is inaccurate or misleading. School personnel may change the education records upon review. If the results are unsatisfactory, parents and eligible students may pursue the formal remedies defined in FERPA.

---

Generally, schools must have written permission from the parent or eligible student before releasing any information from a student's education record. However, FERPA allows schools to disclose those records without consent to the following parties under certain conditions:

- School officials with legitimate educational interest including institutions of higher education at the point of application
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes

- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for or on behalf of the school
- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

### **8. A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising**

Most MaiaLearning third-party partners do not get personally identifying student information that would allow them to engage in targeted advertising. The exception, Parchment, does receive pupil records. For the purpose of electronically transmitted transcripts, Parchment is an optional service available to but not required for use by Schools partner districts. However, Parchment does not provide information to third parties for targeted advertising, as defined in their Privacy Policy.

- 
- (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 [*check one*]  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](mailto: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)**

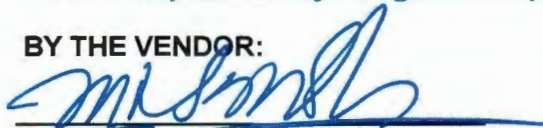
**ERIE 1 BOCES**

**PARENTS BILL OF RIGHTS FOR DATA 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:**

  
Signature

Satish Mirle  
Printed Name

CEO  
Title

Date: **July 29, 2020**

**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, Skills and Strengths Assessments, SAT & ACT Test Prep, and MaiaLearning SEL Curriculum Modules.]

*not  
4/1/22*

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: [Describe steps the Vendor will take]

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 29, 2020] and expires on [June 30, 2023].
- 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.