

## 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

- (e) 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: [Insert here – also provide a copy of Data Security and Privacy Plan]



## Data Security and Privacy Plan

### **Physical Safeguards**

Educational Vistas' programs and data are housed at TurnKey in Latham which is a secure data Center. TurnKey is a 24/7 monitored facility that restricts physical access to the servers. The servers are also appliance and firewall protected from outside access. There are only 3 of our technicians allowed into the data center and the data center is required to call our offices before granting anyone access to the servers. The center requires physical sign-in to the facility as well. Data is housed on multiple redundant load-balanced servers within the facility. Backed up data is encrypted and has to be restored to the data center before it can be used.

### **Encryption in Motion**

The data center uses *https://* to encrypt the data to and from the end points.

### **Encryption at Rest**

Data at rest refers to data that is not moving, data on a drive, or backed up data. For example, this may be a file from a customer. Our internal policies restrict us from putting any client data on a laptop, or USB, or personal devices. Client data can only be accessed through the secure server. Any backed up data is encrypted and cannot be accessed without being restored to the data center.

### **Staff Training related to the Law(s)**

Staff is instructed and trained to not store, remove, or share any customer data. We only use the customer's information in training the customer at the customer's site. Staff is trained on HIPAA Privacy, Security Rules, GLBA, which talks about safeguard procedures against fraud or identity theft and instruction about computer security, and FISMA (Federal Information and Security). We also comply with FERPA, which includes hiring contractors to minimize security risks. Every employee and contractor is required to sign a confidentiality agreement as part of their employment package.

### **Breach Plan and Notification Process**

Our IT security company WLS monitors the servers for Security related Breaches. We require immediate Notification of any security breach so we can in turn immediately notify our clients that a breach has occurred, and what was breached. We have, to this date not had any security breach.

### **Process and Policy to restrict data access to only those with educational interest**

The login and security policies within the program restrict access to the data to individuals that need access to the data. The district will specify to us who is allowed to access the information in the programs. The district also has the ability to change the level of access individuals have within the programs. Normal access is program dependent, e.g. teachers see own students, principals their building, etc. Educational Vistas can also use secure LDAP to allow the

district's active directory server to provide an additional restriction on top of the security the programs provide.

#### **Data Disclosure (Statement of Use)**

Educational Vistas does not use client data. Client data is the property of the client. We do not share client information or client data with anyone. In our services to client district we use client data within the programs for many reasons. Examples would be: To show a teacher which students missed specific standards, print student answer sheets for assessments, build Teacher SLOs, spin assessment data by student for use for teacher driven professional learning, use disaggregated data to set target scores for the district, for the districts to do state reporting like the Civil rights reports, VADIRS, DASA, Discipline Reporting, parent communication templates or to assist setting initial RTI goals based on assessment scores.

#### **Data return or destruction upon end of contract or contract termination**

Educational Vistas will remove all customer data from our servers after receiving a written request from the customer to do so. We will also allow the customer to download extracts of the data before we remove it.

#### **Security protocols related to any subcontractors**

Subcontractors are required to adhere to the same level of security as our internal staff. We require contractors to sign documents stating they will safeguard the data and not use or share any of the districts data.

#### **Ability to Challenge Data Accuracy**

Much of the data we house comes from outside systems such as the district's Student Information System (SIS). We do have the ability to validate data on import to our system(s) and send email notifications to someone at the district that data may be missing that could cause inaccurate reporting to occur. Our Data Sync tool does this automatically if the district wants it. In the StaffTrac APPR system, where evidence can be entered by multiple users, the district can turn on the ability for the data to be user-, time-, and date-stamped. In the SafeSchoolsNY program, the system tracks who reported and who recorded each incident. The district also has the ability to change their own information in order to correct anything that is not accurate. We make it our priority to ensure data accuracy within the programs.

- (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 MISA, below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by and in accordance with Section 8 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-Frunk 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-Frunk 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-Frunk or her designee.
- (e) Vendor will consult directly with Michelle Okal-Frunk or her designee 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: Educational Vistas, Inc.

  
Signature

Lukas J. Crowder  
Printed Name

C.E.O.  
Title

June 12<sup>th</sup>, 2020  
Date

## EXHIBIT D (CONTINUED)

### SUPPLEMENTAL INFORMATION

#### ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT BETWEEN ERIE 1 BOCES AND [EDUCATIONAL VISTAS, INC.]

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

[Curriculum Developer™, DataMate Live, DataMate-DataMate Live-Elite, Social Emotional Learning System (SELS), AIMS, Teacher Evaluation and SLO Tracking 2020]

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: *[EVI will not utilize subcontractors]*

#### **Duration of MLSA and Protected Data Upon Expiration:**

- The MLSA commences on [July 1, 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.