

DATA SHARING AND CONFIDENTIALITY AGREEMENT
BETWEEN
ERIE 1 BOCES AND EDUCATIONAL VISTAS, INC.

This Data Sharing and Confidentiality Agreement (“DSC Agreement”) is made and entered into by and between Educational Vistas, Inc. (“Vendor”), having its principal offices at 2200 Maxon Rd Ext., Schenectady, NY 12308, and the Board of Cooperative Educational Services for the First Supervisory District, Erie County (“Erie 1 BOCES”), having its principal offices at 355 Harlem Road, West Seneca, NY 14224 (collectively referred to as the “Parties”).

1. **Purpose and Term**

(a) **Purpose.** Pursuant to New York General Municipal Law §103(16), Erie 1 BOCES desires to purchase access to Vendor’s software Portfolio(+), and any related support services (“Product”) from Vendor under a Sole Source Agreement.

Erie 1 BOCES will offer access to Vendor’s software Portfolio(+), and any related support services to its component school districts, and school districts located within the jurisdiction of the Western New York Regional Information Center (WNYRIC) that enter into an applicable cooperative service agreement with Erie 1 BOCES (“Participating Educational Agencies”). As a result, Vendor will receive certain personally identifiable information (“PII”) about students and/or teachers and principals from the Participating Educational Agencies that is subject to the provisions of New York State Education Law Section 2-d and Part 121 of the Regulations of the NYS Commissioner of Education (collectively referred to herein as “Section 2-d”).

This DSC Agreement is entered into between Erie 1 BOCES and Vendor in order to conform Vendor’s receipt of PII to the requirements of Section 2-d. This DSC Agreement consists of the terms and conditions set forth herein, a copy of “Erie 1 BOCES Bill of Rights for Data Security and Privacy” signed by Vendor, and the “Supplemental Information about a DSC Agreement between Vendor and Erie 1 BOCES” that is required to be posted on Erie 1 BOCES’ website.

(b) **Term.** By affixing their signatures to this DSC Agreement below, Erie 1 BOCES and Vendor agree that the term of this DSC Agreement shall commence as of the date of mutual execution by the Parties, and shall continue through and until the date of expiration June 30, 2024, or any authorized renewal terms, or, at such time that Erie 1 BOCES has ceased to offer access to Vendor’s software Portfolio(+), and any related support services to any Participating Agencies, whichever is earlier (the “Term”). Vendor shall comply with all terms, conditions and obligations as set forth in this DSC Agreement, including those set forth in Erie 1 BOCES’ Bill of Rights for Data Security and Privacy and the “Supplemental Information about a DSC Agreement between Vendor and Erie 1 BOCES,” throughout the duration of the Term of this DSC Agreement, and this DSC Agreement shall supersede and take the place of any DSC Agreement entered into, or any similar data sharing and confidentiality language previously agreed to by the Parties, prior to the date of mutual execution of this DSC Agreement.

(c) In the event that Vendor has online or written Privacy Policies, End User License Agreements or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of this DSC Agreement, to the extent that any term of the TOS

conflicts with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect.

2. **Definitions**

As used in this DSC Agreement:

(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 Erie 1 BOCES's provision of access to Vendor's software Portfolio(+).

(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 Erie 1 BOCES's provision of access to Vendor's software Portfolio(+).

(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 technology services and software through a Cooperative Educational Services Agreement ("CoSer") with Erie 1 BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the Sole Source Agreement. For purposes of this DSC Agreement, the term also includes Erie 1 BOCES if licensed to use Vendor's Product pursuant to the Sole Source Agreement to support its own educational programs or operations.

(e) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1."

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to Erie 1 BOCES's provision of access to Vendor's software Portfolio(+) may originate from several Participating Educational Agencies located within 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 all Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d), Erie 1 BOCES' policy on data security and privacy, and this DSC Agreement, as may be amended by the Parties. Erie 1 BOCES will provide Vendor with a copy of its policy upon request.

4. **Vendor's Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data it receives from Participating Educational Agencies in accordance with Erie 1 BOCES' 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 DSC 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 DSC 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) As contained in the NIST Cybersecurity Framework, in order to protect the security, confidentiality and integrity of the Protected Data that it receives pursuant to Erie 1 BOCES's provision of access to Vendor's software Portfolio(+), Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the Term of this DSC Agreement:

Data Security:

- Data-at-rest & data-in-transit is encrypted
- Data leak protections are implemented

Information Protection Processes and Procedures:

- Data destruction is performed according to contract and agreements
- A plan for vulnerability management is developed and implemented

Protective Technology:

- Log/audit records are ascertained, implemented, documented, and reviewed according to policy
- Network communications are protected

Identity Management, Authentication and Access Control:

- Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized devices, processes, and users
- Remote access is managed

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about a DSC Agreement between Vendor and Erie 1 BOCES," 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 X will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations resulting from Erie 1 BOCES' purchase of its Product. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations resulting from Erie 1 BOCES' purchase of its Product, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in the "Supplemental Information about a DSC Agreement between Vendor and Erie 1 BOCES," 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 DSC Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data as more fully described in the "Supplemental Information about a DSC Agreement between Vendor and Erie 1 BOCES," 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 terms of this DSC 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 resulting from Erie 1 BOCES' purchase of its Product.

(c) Not use Protected Data for any purposes other than those explicitly authorized in this DSC 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 to Erie 1 BOCES and/or to its Participating Agencies under this DSC Agreement, 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 Protected Data in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in the "Supplemental Information about a DSC Agreement between Vendor and Erie 1 BOCES," 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 DSC 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 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 Joann Lukasiewicz, Manager, Erie 1 BOCES/WNYRIC directly by email at jlukasiewicz@e1b.org, or by calling 716-821-7126.

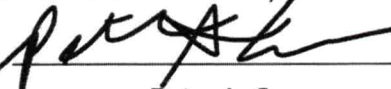
(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Joann Lukasiewicz or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, 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 Erie 1 BOCES or its Participating Districts if they have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES 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 Joann Lukasiewicz or his/her designee.


(e) Vendor will consult directly with Joann Lukasiewicz or his/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.

IN WITNESS WHEREOF, the Parties have caused this DSC Agreement to be executed by their duly authorized representatives as of the dates set forth below.

EDUCATIONAL VISTAS, INC.

By: 
Printed Name: Peter A. Cooper
Title: National Sales Manager
Date: 8/10/2023

ERIE 1 BOCES

By: 
Printed Name: Jim Frayette
Title: Exec. Director
Date: 8/22/23

DATA SHARING AND CONFIDENTIALITY AGREEMENT (CONTINUED)

ERIE 1 BOCES

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:



Signature

National Sales Manager

Title

8/10/2023

Date

DATA SHARING AND CONFIDENTIALITY AGREEMENT (CONTINUED)

SUPPLEMENTAL INFORMATION ABOUT A DATA SHARING AGREEMENT BETWEEN EDUCATIONAL VISTAS, INC. AND ERIE 1 BOCES

Erie 1 BOCES purchases certain software and related support services, as more fully described below.

Portfolio(+)

Participating Educational Agencies (*i.e.*, those educational agencies that are authorized to use the above Product(s) by purchasing certain shared technology services and software through a Cooperative Educational Services Agreement with Erie 1 BOCES) 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"). Educational Vistas, Inc. has entered into a Data Sharing and Confidentiality Agreement ("DSC Agreement") with Erie 1 BOCES setting forth Educational Vistas, Inc.'s obligations to protect the confidentiality, privacy and security of Protected Data it receives as a result of Erie 1 BOCES' purchase of its Product.

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Educational Vistas, Inc. is being provided access to the Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Educational Vistas, Inc. agrees that it will not use the Protected Data for any other purposes not explicitly authorized above or in the DSC Agreement. Protected Data received by Educational Vistas, Inc., or any of Educational Vistas, Inc.'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 Educational Vistas, Inc. engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations resulting from Erie 1 BOCES' purchase of its Product (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Educational Vistas, Inc. under the DSC Agreement and applicable state and federal law. Educational Vistas, Inc. will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Subcontractors at Educational Vistas, 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 data.

Duration of DSC Agreement and Protected Data Upon Expiration:

- The DSC Agreement shall continue through and until the date of expiration June 30, 2024, or any authorized renewal terms, or, at such time that Erie 1 BOCES has ceased to offer access to Educational Vistas, Inc. software Portfolio(+), and any related support services to any Participating Agencies, whichever is earlier. Upon expiration of the DSC Agreement without renewal, or upon termination of the DSC Agreement prior to expiration, Educational Vistas, Inc. will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Educational Vistas, Inc. 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, Educational Vistas, Inc. 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.

- Educational Vistas, Inc. will cooperate with Erie 1 BOCES as necessary to transition Protected Data to any successor Vendor prior to deletion.
- Neither Educational Vistas, Inc. 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, Educational Vistas, Inc. 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 Educational Vistas, Inc., 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 any APPR data provided to Educational Vistas, Inc. by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Educational Vistas, Inc. receives will be stored on systems maintained by Educational Vistas, Inc., or by a subcontractor under the direct control of Educational Vistas, Inc., in a secure data center facility located within the United States. The measures that Educational Vistas, Inc. 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: Educational Vistas, Inc. (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.



INCREASING EFFICIENCY.
REDUCING COSTS.

Educational Vistas, Inc.

2200 Maxon Rd. Ext.
Schenectady, NY 12308
(518) 344-7022

Data Privacy and Security Statement

Parent Bill of Rights for Data Privacy and Security

Educational Vistas, Inc. complies with and exceeds all expectations of Section 2-c and 2-d of the Education Law.

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 SHA-256 bit encryption along with *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.



Educational Vistas, Inc.

2200 Maxon Rd. Ext.
Schenectady, NY 12308
(518) 344-7022

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.

LUKAS J. CROWDER - CFO

(Authorized Representative)

(Signature)

SUPPLEMENTAL INFORMATION

Complete the chart below with information required to post about the contract, along with our parent bill of rights.

SUPPLEMENTAL INFORMATION ELEMENT	2-D	121	SUPPLEMENTAL INFORMATION
The exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract	3(c)	3(c)	To support and enhance the use of licensed products and services each year.
How the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract	3(c)	3(c)	EVI will not share any protected data with any other entities.
When the agreement expires and what happens to the protected data when the agreement expires	3(c)	3(c)	All data will be housed, secured, and maintained until such a time as the licensor requests it's removal from our servers in writing.
If a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how	3(c)	3(c)	All directives for the changing of data will come from the licensor's administrator(s) and not from Parents / Students directly. If contacted directly, EVI will refer all Parents / Students to the licensor.
Where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated	3(c)	3(c)	Our servers are housed at Turnkey Internet - Data Center & Cloud Hosting Solutions, 175 Old Loudon Rd, Latham, NY 12110. This facility has 24/7 physical safeguards in place, along with redundancy measures and load balancing.
How the data will be protected using encryption.	3(c)	3(c)	SHA-256 Encryption