BROOME•TIOGA
boces
Enriching Lives Through Education

Broome-Tioga BOCES
Parents' Bill of Rights for Data Privacy and Security

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

- A student's personally identifiable information cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's education record.
- 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.
- 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 Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- 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, NY, 12234. Complaints may also be directed to the Chief Privacy Officer via email at: privacy@nysed.gov.
- The BOCES will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information.

Appendix
Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Broome-Tioga BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data" as those terms are defined by law.

Each contract BOCES enters into with a third-party contractor, where the third-party contractor receives student data or teacher or principal data, will include the following information:

- The exclusive purposes for which the student data or teacher or principal data will be used.
- How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
- When the agreement expires and what happens to the student data or teacher orprincipal data upon expiration of the agreement.
- If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected.
- Where the student, teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

This section to be completed by the Third-Party Contractor and returned to Broome-Tioga BOCES

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

☑ Yes
Please complete Sections 2, 3 and 4

□ No
Please complete Section 3

Section 2: Supplemental Information Details
Third-Party Contractors subject to New York Education Law § 2-d – please complete the table below

SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list 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 (or list the section(s) in the contract where this information can be found)	See Attachment
Please list 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 (or list the section(s) in the contract where this information can be found)	See Attachment
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	See Attachment
Please list how 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 (or list the section(s) in the contract where this information can be found)	See Attachment
Please list 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 (or list the section(s) in the contract where this information can be found)	See Attachment
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	See Attachment

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the terms of Broome-Tioga BOCES Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

Company Name: Educational Vistas, Inc.

Product Name: Portfolio (+) Archive only

Printed Name: Lukas J. Crowder

Signature ____________

Date 8/24/22

Section 4: Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

BOCES and the Third-Party Contractor agree as follows:

1. Definitions:
   a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
   b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the BOCES's Data Security and Privacy Policy;

3. The Parties agree that the BOCES's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
   a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
   b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
   c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
      i. without the prior written consent of the parent or eligible student; or
      ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
   d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
   e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
   f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
   g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Educational Vistas, Inc.   Product Name: Portfolio (+) Archive only

Printed Name: Lukas J. Crowder   Signature ____________ Date 8/24/22

Educational Vistas, Inc.

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.

EV Educational Vistas, Inc.

INCREASING EFFICIENCY.
REDUCING COSTS.

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