

Schedule “F”
New York Education Law 2-d

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 or principal 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 |
|--|---|
| <p>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)</p> | <p>We do not share student data or teacher or principal data with any third-party contractors.</p> <p>The exclusive purpose for which Vendor is being provided access to the Protected Data is to provide Participating Educational Agencies with the functionality of eTrition. Vendor 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 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.</p> |
| <p>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)</p> | <p>In the event that Vendor engages subcontractors, assignees, or other authorized persons or entities, 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 Vendor under the Contract and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements. Harris Computer does not utilize subcontractors</p> <p>Harris does not share any protected data with any third party, unless it is initiated by the customer. All data is housed in a secure environment that by design complies with the data protection and security provisions of law, regulation and this contract.</p> |
| <p>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)</p> | <p>If the agreement were to expire, customers will have the option to purchase a read-only access to all of their data, for as long as they require. In any case all data is securely backed up, and can be restored upon request by a former customer that requires read-only access or desires a new agreement.</p> |
| <p>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)</p> | <p>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 any APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.</p> |
| <p>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)</p> | <p>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.</p> <p>Protected data is stored in a SQL server database, unique per customer, and it is hosted in the "Cloud" by Expedient. The physical location is highly secured and is staffed 24x7x365. Database backups are also stored within Expedient's cloud platform, using Cohesity for management. The facility is closed to the public. The virtual environment is secured behind a Harris VPN, and</p> |


| | |
|--|---|
| | only personnel with granted rights have access to the environment to perform maintenance. |
| Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found) | <p>Database: Personal Identifiable Information (PII) is encrypted using AES-256, in combination with a strong unique key.</p> <p>Connection Encryption: all customer traffic to and from eTriton utilizes an end-to-end SSL encryption. We also utilize Cloudflare which provides Web Application Firewall solution and strengthen the data traffic encryption for the older devices that does not support the latest SSL/TLS.</p> <p>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.</p> |

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: N. Harris Computer Corporation Product Name: eTriton

Printed Name Marc Keller Signature  Date 12/7/2021

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: N. Harris Computer Corporation Product Name: eTriton

Printed Name Marc Keller Signature  Date 12/7/2021