



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.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, 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.
- 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 directed to the chief privacy officer via email at: CPO@mail.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
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)	The student or teacher data will be used to provide service.
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)	Heartland does not share protected data within any other entity.
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)	Heartland agrees to destroy protected data within a reasonable time period after the contract ends or is terminated. This business process is managed within the scope of safeguarding the protected data stored for business purposes or regulatory purposes.
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)	Parents have the right to challenge the accuracy of the student data that is collected by Heartland. Any such challenge must be submitted, in writing, to: Heartland School Solutions Attn.: MySchoolBucks Support 765 Jefferson Rd, Suite 400 Rochester, NY 14623
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)	Data supporting Heartland Hosted Applications such as MySchoolBucks.com or Mosaic is stored in our co-location facilities in two different regions of the continental US. Consistent with industry standards, Heartland applies PCI DSS guidelines to secure confidential data. As prescribed by the PCI DSS framework, Heartland implements the following initiatives to address data security issues, including access, data storage, privacy and protection.

However, no precautions, means, or method of transmission which uses the internet is absolutely 100% secure. For these reasons, Heartland cannot guarantee absolute security of your confidential data.

1. Install and keep updated a firewall between the public network and the confidential information.
2. Change vendor-supplied passwords that come with network and information processing systems.
3. Safeguard the confidential data stored for business purposes or regulatory purposes.
4. Encrypt all transmissions of customer data over any public network.
5. Maintain antivirus software in all of your computers.
6. Develop and maintain secure systems and applications.
7. Limit access to the confidential data to as few people as possible on the "need-to-know" basis within your business.
8. Identify and authenticate access to system components.
9. Restrict physical access to the systems.
10. Track and monitor access to network resources and confidential data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)

a. End-users transmit information over Internet using HTTPS SSLv3 / TLS 1.2 connections encrypted with at least RC4/AES-128 bit stream ciphers based encryption.

	<p>b. MySchoolBucks encrypts cardholder information using an internal 'Voltage' encryption / key management device and stores the encrypted values in a SQL Server database.</p> <p>c. The SQL Server database is stored on a Pure Storage SAN device that uses 256-bit AES encryption</p>
--	--

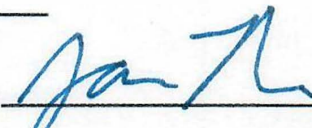
Section 3: Agreement and Signature

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 Heartland Payment Systems LLC, dba Heartland School Solutions

Product Name MySchoolBucks

Printed Name Jeremy Loch Signature  Date 6/9/20

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 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 if 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 authorized 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 Heartland Payment Systems LLC, dba Heartland School Solutions

Product Name MySchoolBucks

Printed Name Jeremy Loch

Signature



Date 6/9/20