C. Successful Vendor agrees to comply with the requirements of New York State Education Law §2-d and Eastern Suffolk BOCES confidentially requirements, both fully described in the rider attached hereto as Attachment "C."

Please reference, in the following pages, the documents outlined below:

- Attachment C-Education Law 2-d Rider
- Data Security and Privacy Plan
    - Heartland Levels of Security Overview
    - Heartland Data Security & Privacy Plan
- ESBOCES Parents' Bill of Rights for Data Security and Privacy

Attachment C-Education Law 2-d Rider

Attachment C

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Heartland Payment Systems, LLC dba Heartland School Solutions (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to personally identifiable: student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts that ESBOCES and/or the participating school district has identified to Contractor in writing as sensitive or confidential data of ESBOCES and/or the participating school district. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall delete all of ESBOCES' and/or participating school districts' Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option, or direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, ESBOCES or the institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

<CONTRACTOR>

BY: _____ **DATED:** April 10, 2025

Jeremy Loch/President, Schools and Communities
Heartland Payment Systems, LLC dba Heartland School Solutions

***Please reference the "Heartland's Exceptions to RFP Documentation" section of our response for additional information.

***Please reference the "Heartland Levels of Security Overview" + "Heartland Data Security & Privacy Plan" section(s) of our response for additional information.

Data Privacy and Security Plan

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

***Please reference the "Heartland Levels of Security Overview" + "Heartland Data Security & Privacy Plan" section(s) of our response for additional information.

Heartland Levels of Security Overview

Mosaic Cloud Security

Heartland provides hosted services to more than 100,000 clients and employs numerous data security measures that are continually audited for compliance at the highest level. With Mosaic Cloud, you will not only be able to access program data anywhere there is an internet connection, but you will also receive world-class data protection 24/7.

Heartland's Processes for Secure Data Protection

Build and Maintain a Secure Network	■ Install and maintain a firewall configuration. ■ Change vendor supplied passwords and security parameters.
Safeguard Data	■ Protect customer data stored for business or regulatory purposes. ■ Encrypt all transmissions of customer data over public networks.
Maintain a Vulnerability Management Program	■ Maintain current antivirus software on all computers. ■ Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	■ Restrict access to customer data on a need to know basis. ■ Require unique user ID for access to customer data. ■ Restrict physical access to stored data.
Regularly Monitor and Test Networks	■ Track and monitor all access to networks and data. ■ Regularly test security applications.
Maintain an Information Security Policy	■ Maintain employee training and information security policies.

Data Protection

Heartland employs numerous software packages to protect your district data:

- Microsoft SQL Server manages data, controls access, regulates data viewing/modification.
- Microsoft Windows Server provides the next line of defense by managing the network, including authentication and authorization. Employees with access to the database are regularly reviewed by an audit group.
- The data center utilized multiple tools to monitor network, server infrastructure, database and storage layers 24/7.
- Routers/Network Firewalls, Intrusion detection, Application Firewalls and Virus Scans are also employed.
- Data-at-rest is encrypted.

Certification & Compliance

Heartland's data center is audited for compliance with Statement on Standards for Attestation Engagements (SSAE) 16.

The Heartland data security team holds the following credentials:

- Certified Information Systems Security Professional (CISSP)
- Certified Payment-Card Industry Security Auditor (CPISA/M)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- IT Service Management (ITSM)
- Project Management Professional (PMP)
- Certified Ethical Hacker (CEH)

Business Continuity Procedures

Heartland's hosting service resides in a Tier 4 facility- the highest standard in data center security. Our data centers are located in the continental United States and feature:

- Business access managed by a security force.
- Multiple independent distribution paths that serve IT equipment.
- Dual-powering of all IT equipment.
- Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of at least 99.999%
- Independently dual-powered cooling equipment, including chillers and heating, ventilating, and air-conditioning (HVAC).

Disaster Recovery Strategy

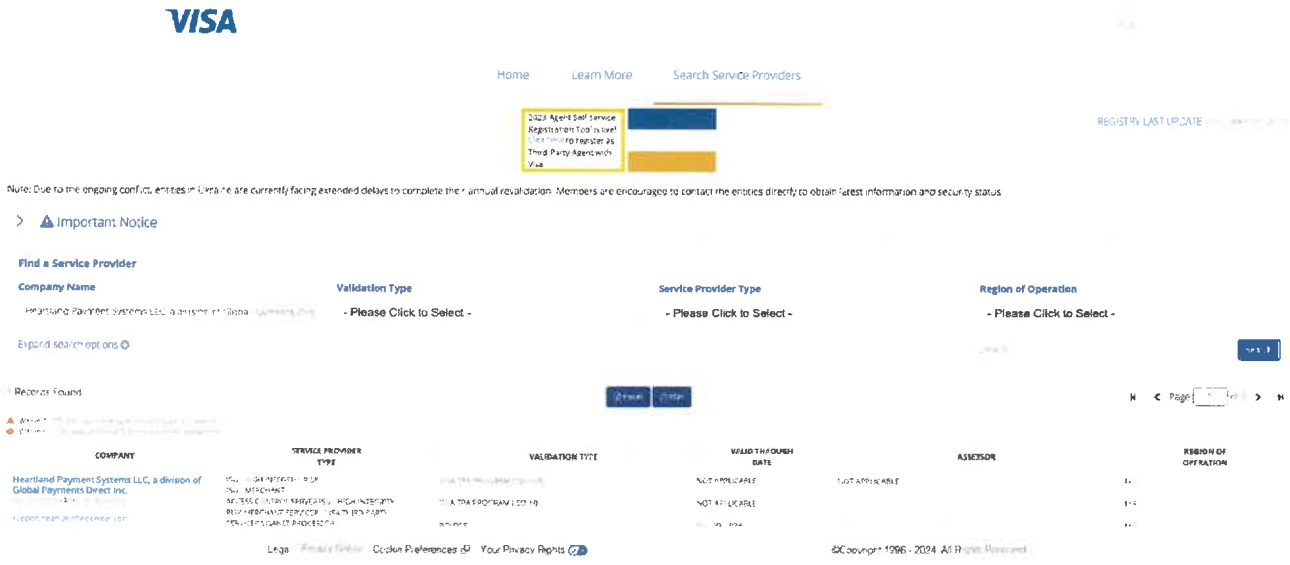
Heartland maintains a Disaster Recovery environment, with existing data pipes between data centers. Our high-level strategy is as follows:

- User Border Gateway Protocol (BGP) to manage the switch to/from the Disaster Recovery environment.
- Test Disaster Recovery readiness on an annual basis.
- Establish an asynchronous mirror of the production dataset:
    - Use the Availability Groups functionality with SQL Server
    - The mirrored instance of the database will be located in the DR environment

MySchoolBucks Security

Heartland's Security Office maintains oversight on our compliance, audit and service offerings. As such, the security office is engaged in all major software design and service decisions, from design through deployment.

Heartland is also certified at PCI Service Provider Level 1. This certification can be validated by visiting the Visa Global Registry of Service Providers, found on the Internet at: http://www.visa.com/splisting/.



PCI & Security

Heartland is committed to providing our clients and your customers with superior technology and world-class security. Our proposed solution has been certified to the PCI-DSS Level 1 security standard at the Service Provider Level. Heartland's front and back-end platforms utilize strong encryption and rigorous key management protocols. In conjunction with data encryption measures, Heartland uses a defense-in-depth approach to monitor our infrastructure and applications against malicious and potentially fraudulent activity.

As a Service Provider Level 1 entity, Heartland is subjected to a more rigorous set of obligations for compliance. Among other things, this distinction means that Heartland's controls are subjected to an on-site assessment by a third-party Qualified Security Assessor rather than merely completing a self-assessment questionnaire.

From Heartland's perspective, the importance of maintaining secure systems, as well as PCI certification, cannot be overstated. As such, Heartland is committed to meeting its current obligations for PCI Compliance as well as future obligations that emerge as new PCI requirements are promulgated. Not only is Heartland PCI compliant, but also it is a member of the PCI Security Standards Council.

Heartland is committed to being a thought leader in the industry. In partnership with the Financial Services Information Sharing and Analysis Center (FS-ISAC), Heartland helped create the Payments Processing Information Sharing Council (PPISC), an industry forum for sharing sensitive (and oftentimes non-public) information about fraud, threats, vulnerabilities, and risk mitigation practices within the payments industry.

Please reference the "Data Section" of our website utilizing the link below for additional information: https://www.heartlandpaymentsystems.com/data-security.

Platform Performance & Disaster Recovery

Our established service level operating objective is 99.999% uptime, which is based on our experience in serving a large pool of national merchants. The Heartland's application has certainly achieved this objective over the past 6 months, and we regularly exceed this objective. Heartland operates its front-end processing, back-end processing, and other hosted product offerings in two geographically-dispersed data centers located within the continental United States. Heartland leverages both of these data centers to deliver highly available and secure platforms. Data integrity and multi-site readiness are achieved using data replication techniques. Transactions are mirrored between the data centers, and each center has the capacity to handle our full merchant transaction load. Heartland leverages this redundant processing capability to deliver on its uptime commitments, and we regularly process through both data centers.

Heartland's application is designed and configured to be fully redundant, with multiple web and app servers that are available and load balanced with our app directors. Multiple monitoring solutions are in place, with external user experiences from multiple US cities using WebMetrics and/or Azure. Internal monitoring is through Logic Monitor.

From a Disaster Recovery perspective, we manage this through an AlwaysOn SQL which is not dependent upon any form of shared storage. We do this while also having local and multi-region failovers, ensuring overall redundancy and high availability. Our data is also encrypted at rest and replicated over a secure tunnel. We have dedicated security and performance teams monitoring 24/7 within our own NOCs, ready to respond instantly to any security issues. In the event of a regional outage, our disaster recovery plan, including BGP failover, ensures minimal disruption. Plus, we test our recovery processes regularly to maintain peak performance. All of this means that the data stays secure, the services remain reliable, and everything stays running without interruption.

Heartland's MySchoolBucks platform is a hosted solution. If there is a disaster impacting power and/or communication systems, Heartland's documented response plans envision a return to normal operation within minutes by leveraging QWEST BGP as well as our alternate data center.

Defenses Against Cyberattacks

Located within the continental United States, Heartland's Security Intelligence Operations Center (SIOC) is a 24/7 operation with responsibility for monitoring, detecting, remediating and reporting on security events and incidents across the Heartland enterprise. The SIOC's primary responsibility is to ensure that security events and incidents are detected and handled in a timely manner. The events that they monitor come from the logs of virtually every device on the network—servers, firewalls, routers, PCs, etc. These events are correlated by a Security Information and Event Management system, along with information from various security threat intelligence sources, into actionable alerts. Through their various tools and processes, the SIOC helps to remediate identified security and operational issues.

Heartland Data Security & Privacy Plan

Purpose

The purpose of this document is to describe the plan for ensuring that confidential data entrusted to Heartland School Solutions ("HSS") remains secure.

Scope

This plan applies to the District's confidential data that is stored within the MySchoolBucks and Hosted MCS and Mosaic systems. To the extent District has the installed version of HSS software, District is responsible for the information security of its data.

Executive Summary

HSS maintains industry standard administrative, technical and physical safeguards to protect the confidentiality of information transmitted online, including but not limited to encryption, firewalls, password protection, and SSL (Secure Sockets Layer). HSS has implemented policies and practices that reflect a variety of security standards, as well as applicable laws and regulations, relating to the security and safeguarding of confidential data. However, no precautions, means, transmission using the internet, or storage system is absolutely 100% secure. For these reasons, HSS cannot guarantee absolute security of the District's confidential data.

Sharing Confidential Data

HSS complies with the limitations in FERPA, and does not share student data with any third party for marketing or advertising purposes. HSS uses confidential data only for the purposes identified in the agreement with the District. Such purposes may require that the confidential data be shared with third parties, including financial entities that facilitate the flow of funds to/from the District. HSS also complies with all applicable state laws, including New York's Education Law and the California Consumer Privacy Act.

Parents' Bill of Rights

HSS may enter into agreements with District-authorized parents, guardians, or other users accessing the MySchoolBucks site (collectively "MySchoolBucks Parents"). Notwithstanding any provision of the agreement between MySchoolBucks Parents and HSS to the contrary, HSS adheres to the following Parents' Bill of Rights:

1. HSS will not sell or release a student's personally identifiable information for any commercial purpose.
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 HSS uses safeguards associated with industry standards and best practices, including but

not limited to, encryption, firewalls, and password protection, when data is stored or transferred by HSS.

4. A complete list of all student data elements stored within the relevant software will be made available upon request.
5. Parents have the right to make complaints about possible breaches of student data. Such complaints should be sent to the postal address listed under Contact Us in the Privacy Policy on the MySchoolBucks website, located at https://www.myschoolbucks.com/ver2/etc/getprivacy.

Implementation – Data Security

HSS has implemented numerous security initiatives designed to ensure compliance with applicable laws and contracts regarding data security. Our internal control processes are audited for SSAE 18 certification, and we are certified as a Level 1 Service Provider with the Payment Card Industry Data Security Standards ("PCI DSS"). PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. HSS engages a third-party Qualified Security Assessor for annual PCI compliance audits. Both the District and HSS need to certify PCI-DSS compliance to accept and process credit and debit card payments.

PCI DSS includes the following requirements:

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 robust antivirus software in all systems.
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.

Other Data

MySchoolBucks Parents may supply data, including confidential data, to utilize the MySchoolBucks service. The MySchoolBucks Terms of Use and Privacy Policies govern the sharing of data supplied by MySchoolBucks Parents.

ESBOCES Parents' Bill of Rights for Data Security and Privacy

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.

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.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 to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk 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." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

See attached two pages for answers to these questions -

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   Answer: *The successful vendor needs to confirm that any and all data (including student, teacher, and principal data) is not to be used for any purpose, other than the encryption of that data.*

2. 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;

   Answer: *The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements.*

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   Answer: *The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements at the expiration of the agreement.*

4. 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; and

   Answer: *Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:*

   Claudy Damus-Makelele, Associate Superintendent for Educational ServicesEastern Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772
   cdamus@esboces.org;

   Or in writing to:

   Chief Privacy Officer, New York State Education Department, 89 Washington Avenue
   Albany, NY 12234
   CPO@mail.nysed.gov

5. Where the student data or 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.

   Answer: *The successful vendor will be required in the bid process to describe how they will ensure data is encrypted and protected.*

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose 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 third-party contractor provides a 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 the statute or court order;

5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

***Please reference the "Heartland's Exceptions to RFP Documentation" section of our response for additional information.

The following has been pulled from the Parents' Bill of Rights section in the Education Law 2-d Rider packet. Please review and answer questions 1, 2, 3 and 5.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   Answer: **The data will be used to allow the applications in scope to provide the services intended.**

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

   Answer: **Heartland will ensure that its employees, subcontractors and third-party service providers with whom Contractor shares PII abide by all applicable data protection and security requirements by entering into written agreements whereby such parties will perform their obligations in a manner consistent with the data protection and security requirements outlined therein.**

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   ***Answer*: Upon expiration or termination of the Agreement, Heartland shall:**

   • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.

   • Securely delete and destroy data.

4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected;

   Answer: Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

   Claudy Damus-Makelele, Associate Superintendent for Educational Services Eastern Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772 cdamus@esboces.org ;

   Or in writing to:

   Chief Privacy Officer, New York State Education Department, 89 Washington Avenue Albany, NY 12234 CPO@mail.nysed.gov

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security) and the security protections taken to ensure that such data will be protected, including whether such data will be encrypted.

Answer: **All data is hosted in the US in redundant data centers.**

Consistent with industry standards, Heartland applies PCI DSS guidelines to secure confidential data. As prescribed by the PCS DSS framework, Heartland implements the following initiatives to address data security issues, including access, data storage, privacy and protection. However, no means, or method of transmission which uses the internet is absolutely 100% secure, For these reason, Heartland cannot guarantee absolute security of your confidential data.

Security Practices

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.